

NetIQ® Sentinel™

Installation and Configuration Guide

February 2015

Contents

About this Book and the Library

The *Installation and Configuration Guide* provides an introduction to NetIQ Sentinel and explains how to install and configure Sentinel.

Intended Audience

This guide is intended for Sentinel administrators and consultants.

Other Information in the Library

The library provides the following information resources:

Administration Guide

Provides administration information and tasks required to manage a Sentinel deployment.

User Guide

Provides conceptual information about Sentinel. This book also provides an overview of the user interfaces and step-by-step guidance for many tasks.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

I Understanding Sentinel

This section provides detailed information about what Sentinel is and how Sentinel provides an event management solution for your organization.

1 What is Sentinel?

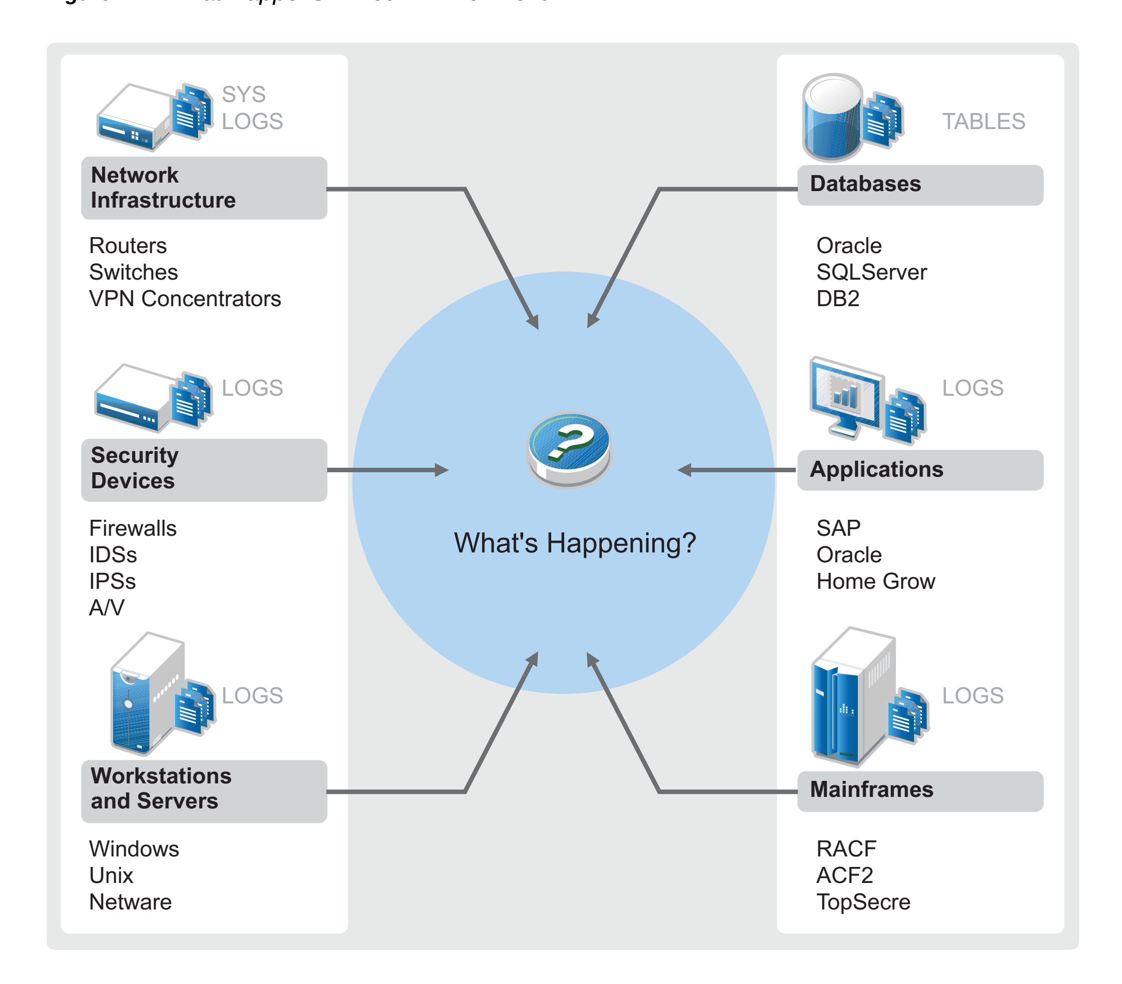
Sentinel is a security information and event management (SIEM) solution as well as a compliance monitoring solution. Sentinel automatically monitors the most complex IT environments and provides the security required to protect your IT environment.

- Section 1.1, "Challenges of Securing an IT Environment," on page 15
- Section 1.2, "The Solution That Sentinel Provides," on page 16

1.1 Challenges of Securing an IT Environment

Securing your IT environment is a challenge due to the complexity of your environment. There are many different applications, databases, mainframes, workstations, and servers that all have logs of events. You also have the security devices and network infrastructure devices that all contain logs of what is happening in your IT environment.

***Figure 1-1** What Happens in Your Environment*



The challenges arise because of the following facts:

- There are many devices in your IT environment.
- The logs are in different formats.
- The logs are stored in silos.
- The amount of information generated in the logs.
- You can’t determine who did what without manually analyzing all of the logs.

To make the information useful, you must be able to perform the following:

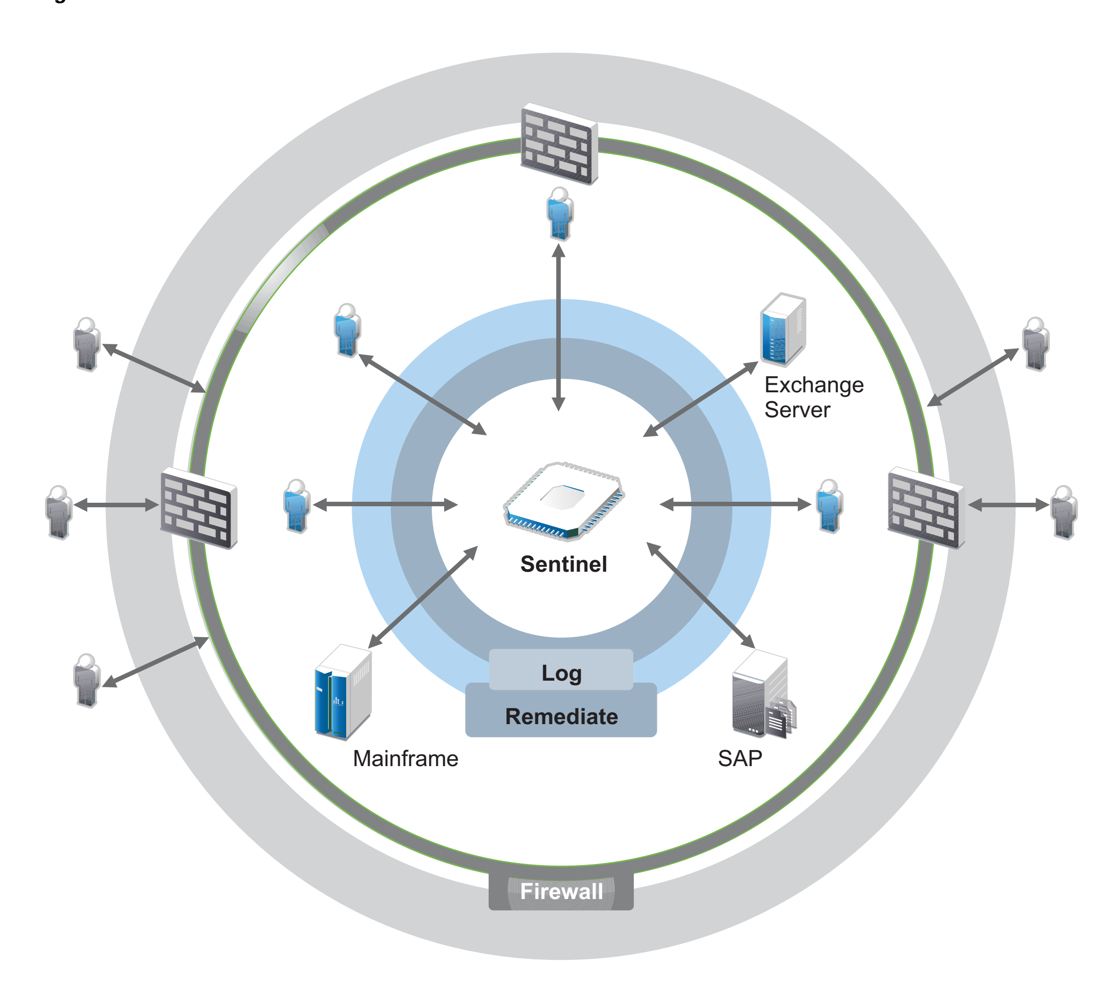
- Collect the data.
- Consolidate the data.
- Normalize disparate data into events that you can easily compare.
- Map events to standard regulations.
- Analyze the data.
- Compare events across multiple systems to determine if there are security issues.
- Send notifications when the data is outside of the norms.
- Take action on notifications to comply with business policies.
- Generate reports to prove compliance.

After you understand the challenges of securing your IT environment, you need to determine how to secure the enterprise for and from users without treating them like malicious users, or burdening them to the point where it is impossible to be productive. Sentinel provides the solution.

1.2 The Solution That Sentinel Provides

Sentinel acts as the central nervous system to the enterprise security. It pulls in data from across your entire infrastructure—applications, databases, servers, storage, and security devices. It analyzes and correlates the data, and makes the data actionable, either automatically or manually.

Figure 1-2 The Solution That Sentinel Provides



The result is that you know what is happening in your IT environment at any given point, and you have the ability to tie the actions taken on resources to the people taking those actions. This allows you to determine user behavior and effectively monitor control. No matter if that person is an insider or not, you can tie together all the actions they take so that unauthorized activities become clear before they do damage.

Sentinel does this in a cost-effective way by:

- Providing a single solution to address IT controls across multiple regulations.
- Closing the knowledge gap between what should happen and what is actually happening in your networked environment.
- Demonstrating to auditors and regulators that your organization documents, monitors, and reports on security controls.
- Providing out-of-the-box compliance monitoring and reporting programs.
- Gaining the visibility and control required to continually assess the success of your organization's compliance and security programs.

Sentinel automates log collection, analysis, and the reporting processes to ensure that IT controls are effective in supporting threat detection and audit requirements. Sentinel provides automated monitoring of security events, compliance events, and IT controls allowing you to take immediate action if there is a security breach or non-compliant event occurring. Sentinel also allows you to easily gather summary information about your environment so you can communicate your overall security posture to key stakeholders.

2 How Sentinel Works

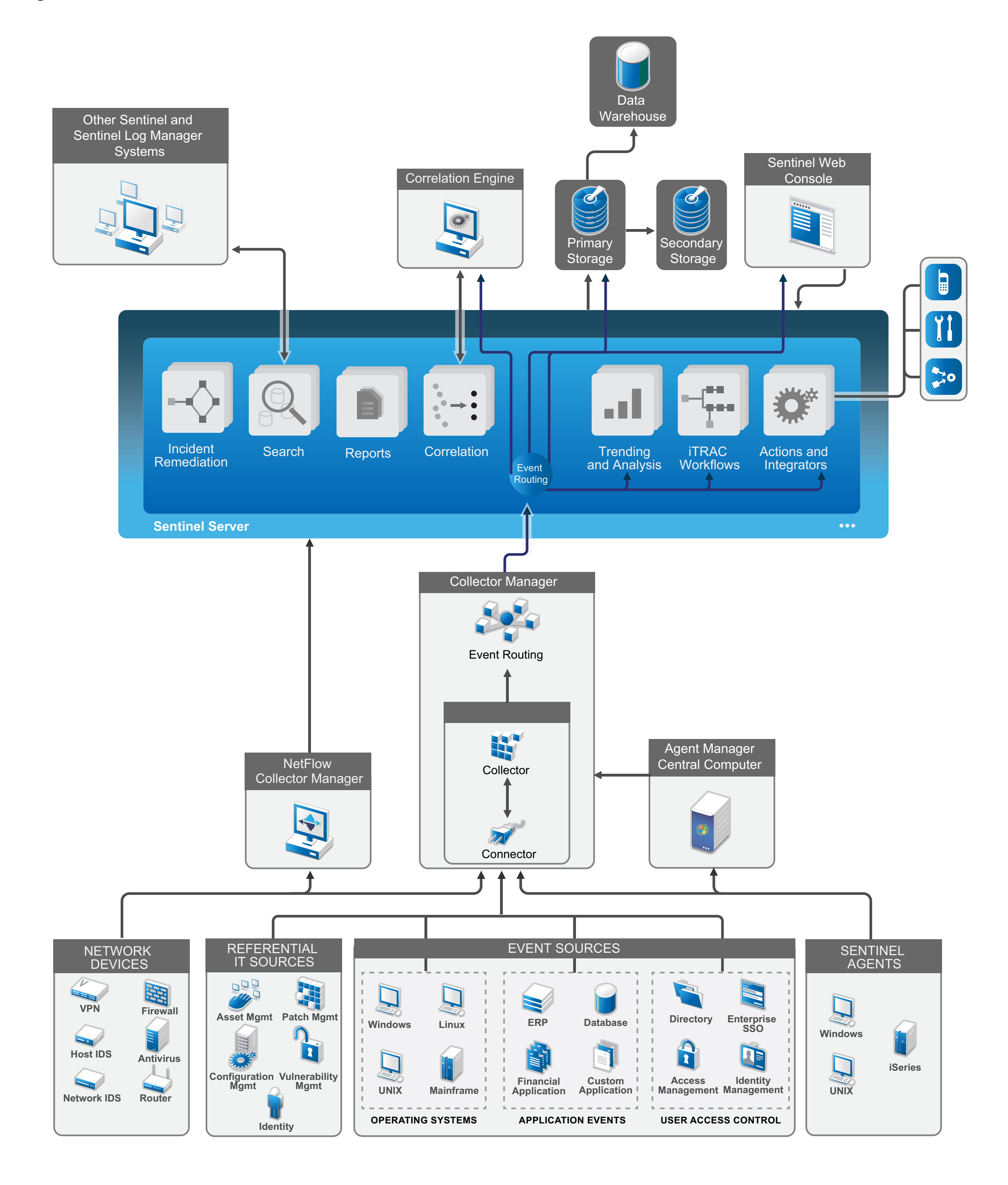
Sentinel continuously manages security information and events throughout your IT environment to provide a complete monitoring solution.

Sentinel does the following:

- Gathers logs, events, and security information from all of the different event sources in your IT environment.
- Normalizes the collected logs, events, and security information into a common format.
- Stores events in a file-based data store with flexible, customizable data retention policies.
- Collects network flow data and helps you monitor network activities in detail.
- Provides the ability to hierarchically link multiple Sentinel systems, including Sentinel Log Manager.
- Allows you to search for events not only on your local Sentinel server, but also on other Sentinel servers distributed across the globe.
- Performs a statistical analysis that allows you define a baseline and then compares it to what is occurring to determine if there are unseen problems.
- Correlates a set of similar or comparable events in a given period to determine a pattern.
- Organizes events into incidents for efficient response management and tracking.
- Provides reports based on real time and historical events.

The following figure illustrates how Sentinel works:

Figure 2-1 Sentinel Architecture



The following sections describe Sentinel components in detail:

* Section 2.1, "Event Sources," on page 21
* Section 2.2, "Sentinel Event," on page 21
* Section 2.3, "Collector Manager," on page 23
* Section 2.4, "Agent Manager," on page 23

2.1 Event Sources

Sentinel gathers security information and events from many different sources in your IT environment. These sources are called event sources. The event sources can be many different items on your network.

Security Perimeter: Security devices including hardware and software used to create a security perimeter for your environment, such as firewalls, IDS, and VPNs.

Operating Systems: Events from the different operating systems running in the network.

Referential IT Sources: The software used to maintain and track assets, patches, configuration, and vulnerability.

Application Events: Events generated from the applications installed in the network.

User Access Control: Events generated from applications or devices that allow users access to company resources.

For more information about collecting events from event sources, see “Configuring Agentless Data Collection”.

2.2 Sentinel Event

Sentinel receives information from devices, normalizes this information into a structure called an event, categorizes the event, and then sends the event for processing. By adding category information (taxonomy) to events, events are easier to compare across systems that report events differently. For example, authentication failures. Events are processed by the real time display, correlation engine, dashboards, and the back end server.

An event comprises more than 200 fields. Event fields are of different types and of different purposes. There are some predefined fields such as severity, criticality, destination IP and destination port. There are two sets of configurable fields: Reserved fields are for Sentinel internal use to allow future expansion and Customer fields are for customer extensions.

Fields can be re-purposed by renaming them. The source for a field can either be external, which means that it is set explicitly by the device or the corresponding Collector, or referential. The value of a referential field is computed as a function of one or more other fields using the mapping service. For

example, a field can be defined to be the building code for the building containing the asset mentioned as the destination IP of an event. For example, a field can be computed by the mapping service using a customer defined map using the destination IP from the event.

2.2.1 Mapping Service

The Mapping Service allows a sophisticated mechanism to propagate business relevance data throughout the system. This data can enrich events with referential information that will provide context that enables analysts to make better decisions, write more useful reports, and write well-thought out correlation rules.

You can enrich your event data by using maps to add additional information such as host and identity details to the incoming events from your source devices. This additional information can be used for advanced correlation and reporting. The system supports several built-in maps as well as custom user-defined maps

Maps that are defined in Sentinel are stored in two ways:

- Built-in maps are stored in the database, updated using APIs in Collector code, and automatically exported to the Mapping service.
- Custom maps are stored as CSV files and can be updated on the file system or via the Map Data Configuration UI, then loaded by the Mapping service.

In both cases, the CSV files are kept on the central Sentinel server but changes to the maps are distributed to each Collector Manager and applied locally. This distributed processing ensures that mapping activity does not overload the main server.

2.2.2 Streaming Maps

The Map Service employs a dynamic update model and streams the maps from one point to another, avoiding the buildup of large static maps in dynamic memory. The value of this streaming capability is particularly relevant in a mission-critical real-time system such as Sentinel where there needs to be a steady, predictive and agile movement of data independent of any transient load on the system.

2.2.3 Exploit Detection (Mapping Service)

Sentinel provides the ability to cross-reference event data signatures with Vulnerability Scanner data. Users are notified automatically and immediately when an attack is attempting to exploit a vulnerable system. This is accomplished through:

- Advisor Feed
- Intrusion detection
- Vulnerability scanning
- Firewalls

Advisor provides a cross-reference between event data signatures and vulnerability scanner data. Advisor feed contains information about vulnerabilities and threats as well as a normalization of event signatures and vulnerability plug-ins. For more information on Advisor, see "Detecting Vulnerabilities and Exploits"in the *NetIQ Sentinel Administration Guide*.

2.3 Collector Manager

The Collector Manager manages data collection, monitors system status messages, and performs event filtering as needed. The main functions of the Collector Manager include the following:

- Transforming events.
- Adding business relevance to events through the mapping service.
- Routing events.
- Determining real-time, vulnerability, asset, or non-real-time data.
- Sending health message to the Sentinel server.

2.3.1 Collectors

The Collectors normalize and collect the information from the Connectors. Collectors are written in JavaScript and they define the logic for the following:

- Receiving raw data from the Connectors.
- Parsing and normalizing the data.
- Applying repeatable logic to the data.
- Translating device-specific data into Sentinel specific data.
- Formatting the events.
- Passing the normalized, parsed, and formatted data to the Collector Manager.
- Device-specific filtering of events.

For more information on Collectors, see Sentinel Plug-ins Web site.

2.3.2 Connectors

The Connectors provide connections from the event sources to the Sentinel system. Connectors use industry-standard protocols to get events such as syslog, JDBC to read from database tables, WMI to read from Windows Event Logs, and so on. Connectors provide:

- Transportation of raw event data from the events sources to the Collector.
- Connection specific filtering.
- Connection error handling.

2.4 Agent Manager

Agent Manager provides host-based data collection that complements agentless data collection by allowing you to:

- Access logs not available from the network.
- Operate in tightly-controlled network environments.
- Improve security posture by limiting attack surface on critical servers.
- Provide enhanced reliability of data collection during times of network interruption

Agent Manager allows you to deploy agents, manage agent configuration, and act as a collection point for events flowing into Sentinel. For more information about Agent Manager, see the Agent Manager documentation.

2.5 NetFlow Collector Manager

The NetFlow Collector Manager collects network flow data (NetFlow, IPFIX, and so on) from network devices such as routers, switches, and firewalls. Network flow data describes basic information about all network connections between hosts including packets and bytes transmitted, which helps you visualize the behavior of individual hosts or the entire network.

The NetFlow Collector Manager functionality includes the following:

- Collects network flow data in bytes, flows, and packets from supported network devices.
- Aggregates and sends the collected data to the Sentinel server for visualization and analysis of network activities in your environment.

For more information about visualizing and analyzing network flow data, see "Visualizing and Analyzing Network Flow Data" in the *NetIQ Sentinel User Guide*.

2.6 Sentinel Data Routing and Storage

Sentinel provides multiple options for routing, storing, and extracting the data collected. By default, Sentinel receives two separate but related data streams from the Collector Managers: the parsed event data and the raw data. The raw data is immediately stored in protected partitions to provide a secure evidence chain. The parsed event data is routed according to rules you define, which you can filter, send to storage, send to real-time analytics, and route to external systems. All event data sent to storage is further matched to user-defined retention policies that determine the partition in which data is placed, and defines the grooming policy under which the event data is retained and then eventually deleted.

Sentinel data storage is based on a three-tier structure:

Online Storage	Primary storage, formerly known as local storage.	Optimized for quick writes and fast retrieval. Stores the most recently collected event data and the most frequently searched event data.
	Secondary storage, formerly known as network storage. (optional)	Optimized to reduce space usage on optionally less expensive storage while still supporting fast retrieval. Sentinel automatically migrates data partitions to the secondary storage.
	NOTE: Using the secondary storage is optional. Data retention policies, searches, and reports operate on event data partitions regardless of whether they are residing on primary or secondary storage, or both.	
Offline Storage	Archival storage	When partitions are closed, you can back up the partition to offline storage such as Amazon Glacier, and similar. If necessary, you can temporarily re-import partitions for use in long-term forensic analysis.

You can also configure Sentinel to extract the event data and event data summaries to an external database by using data synchronization policies. For more information, see "Configuring Data Storage" in the *NetIQ Sentinel Administration Guide*.

2.7 Correlation

A single event may seem trivial, but in combination with other events, it might warn you of a potential problem. Sentinel helps you correlate such events by using the rules you create and deploy in the Correlation engine, and take appropriate action to mitigate any problems.

Correlation adds intelligence to security event management by automating analysis of the incoming event stream to find patterns of interest. Correlation allows you to define rules that identify critical threats and complex attack patterns so that you can prioritize events and initiate effective incident management and response. For more information, see “Correlating Event Data” in the *NetIQ Sentinel User Guide*.

To monitor events according to the Correlation rules, you must deploy the rules in the Correlation Engine. When an event occurs that satisfies the rule criteria, the Correlation Engine generates a correlation event describing the pattern. For more information, see “Correlation Engine” in the *NetIQ Sentinel User Guide*.

2.8 Security Intelligence

The correlation capability in Sentinel provides the ability to look for known patterns of activity, whether it be for security, compliance, or other reasons. The Security Intelligence capability looks for activity that is out of the ordinary, which may be malicious, but does not match any known pattern.

The Security Intelligence feature in Sentinel focuses on statistical analysis of time series data to enable analysts to identify and analyze deviations (anomalies) either by an automated statistical engine or by visual representation of the statistical data for manual interpretation. For more information, see “Analyzing Trends in Data” in the *NetIQ Sentinel User Guide*.

2.9 Incident Remediation

Sentinel provides an automated incident response management system that enables you to document and formalize the process of tracking, escalating, and responding to incidents and policy violations, and provides two-way integration with trouble-ticketing systems. Sentinel enables you to react promptly and resolve incidents efficiently. For more information, see “Configuring Incidents”in the *NetIQ Sentinel User Guide*.

2.10 iTrac Workflows

iTRAC workflows are designed to provide a simple, flexible solution for automating and tracking an enterprise’s incident response processes. iTRAC leverages Sentinel’s internal incident system to track security or system problems from identification (through correlation rules or manual identification) through resolution.

Workflows can be built using manual and automated steps. Advanced features such as branching, time-based escalation, and local variables are supported. Integration with external scripts and plug-ins allows for flexible interaction with third-party systems. Comprehensive reporting allows administrators to understand and fine-tune the incident response processes. For more information, see “Configuring iTRAC Workflows”in the *NetIQ Sentinel User Guide*.

2.11 Actions and Integrators

Actions either manually or automatically execute some type of action, such as sending an email, in Sentinel. Actions can be triggered by routing rules, by manually executing an event or incident operation, and by correlation rules. Sentinel provides a list of preconfigured Actions. You can use the default Actions and reconfigure them as necessary, or you can add new Actions. For more information, see "Configuring Actions" in the *NetIQ Sentinel Administration Guide*.

An Action can execute on its own, or it can make use of an Integrator instance configured from an Integrator plug-in. Integrator plug-ins extend the features and functionality of Sentinel remediation actions. Integrators provide the ability to connect to an external system, such as an LDAP, SMTP, or SOAP server, to execute an action. For more information, see "Configuring Integrators"in the *NetIQ Sentinel Administration Guide*.

2.12 Searching

Sentinel provides an option to perform a search on events. You can search data in the primary storage or the secondary storage location. With the necessary configuration, you can also search system events generated by Sentinel, and view the raw data for each event. For more information, see "Performing a Search"in the *NetIQ Sentinel User Guide*.

You can also search Sentinel servers that are distributed across different geographic locations. For more information, see "Configuring Data Federation"in the *NetIQ Sentinel Administration Guide*.

2.13 Reports

Sentinel provides the ability to run reports on the data gathered. Sentinel is prepackaged with a variety of customizable reports. Some reports are flexible, which allow you to specify the columns to be displayed in the results.

You can run, schedule, and e-mail PDF reports. You can also run any report as a search and then interact with the results as you would do with a search, such as refining the search or performing an action on the results. You can also run reports on Sentinel servers distributed across different geographic locations. For more information, see "Reporting" in the *NetIQ Sentinel User Guide*.

2.14 Identity Tracking

Sentinel provides an integration framework to identity management systems to track the identities of for each user account and what events those identities have performed. Sentinel provides user information such as contact information, user accounts, recent authentication events, recent access events, permission changes, and so on. By displaying information about the people initiating a given action or people affected by an action, incident response times are improved and behavior-based analysis is enabled. For more information, see "Leveraging Identity Information"in the *NetIQ Sentinel User Guide*.

2.15 Event Analysis

Sentinel provides a powerful set of tools to help you easily find and analyze critical event data. The system is tuned and optimized for maximal efficiency in any particular type of analysis, and methods to easily transition from one type of analysis to another are provided for seamless transitions.

Investigating events in Sentinel often starts with the near real-time Active Views. Although more advanced tools are available, Active Views display filtered event streams along with summary charts that can be used for simple, rough analysis of event trends, event data, and identification of specific events. Over time, you build up tuned filters for specific classes of data, such as output from correlation. You can use Active Views as a dashboard showing an overall operational and security posture.

You can then use the interactive search to perform more detailed analysis of events. This allows you to quickly and easily search for and find data related to a specific query, such as activity by a specific user or on a particular system. By clicking on the event data or using the left-hand refinement pane, you can quickly zero in on specific events of interest.

When analyzing hundreds of events, the reporting capabilities of Sentinel provide custom control over event layout and can display larger volumes of data. Sentinel makes this transition easier by allowing you to transfer the interactive searches built up in the Search interface into a reporting template, which instantly creates a report that displays the same data but in a format better suited for a larger number of events.

Sentinel includes many templates for this purpose. Some templates are tuned to display particular types of information, such as authentication data or user creation, and some are general-purpose templates that allow you to customize groups and columns on the report interactively.

Over time, you will develop commonly-used filters and reports that make your workflows easier. Sentinel fully supports storing this information and distributing it with people in your organization. For more information, see the *NetIQ Sentinel User Guide*.

II Planning Your Sentinel Installation

This section guides you through planning considerations before installing Sentinel. If you want to install a configuration that is not identified in the sections that follow, or if you have any questions, contact NetIQ Technical Support.

3 Implementation Checklist

Use the following checklist to complete planning, installing, and configuring Sentinel:

❐	Tasks	See
❐	Review the product architecture information to learn about Sentinel components.	Part I, “Understanding Sentinel,” on page 13.
❐	Review the Sentinel licensing to determine whether you need to use the evaluation license or the enterprise license of Sentinel.	Chapter 4, “Understanding License Information,” on page 33.
❐	Assess your environment to determine the hardware configuration. Ensure that the computers on which you install Sentinel and its components meet the specified requirements.	Chapter 5, “Meeting System Requirements,” on page 37.
❐	Review the Collector Manager and Correlation Engine events per second (EPS), and NetFlow Collector Manager records per second (RPS). Determine the number of Collector Managers, Correlation Engines, and NetFlow Collector Managers you need to install to improve performance and load balancing.	Section 6.1, “Advantages of Distributed Deployments,” on page 39.
❐	Review the Sentinel release notes to understand the new functionality and the known issues.	Sentinel Release Notes
❐	Install Sentinel.	Part III, “Installing Sentinel,” on page 61.
❐	Ensure that you configure the time on the Sentinel server.	Chapter 17, “Configuring Time,” on page 95.
❐	When you install Sentinel, the Sentinel plug-ins available at the time of the Sentinel release are installed by default. Configure the out-of-the-box plug-ins for data collection and reporting purposes.	Chapter 19, “Configuring Out-of-the-Box Plug-Ins,” on page 101.
❐	Sentinel includes correlation rules out-of-the-box. Some correlation rules are configured by default to execute an action that sends an email when the rule fires, such as the Notify Security Admin action. Therefore, you need to configure the mail server settings in the Sentinel server by configuring the SMTP Integrator and the Send Email action.	SMTP Integrator and Send Email action documentation on the Sentinel Plug-ins Web site.
❐	Install additional Collectors and Connectors as needed in your environment.	Chapter 15, “Installing Additional Collectors and Connectors,” on page 89.
❐	Install additional Collector Managers and Correlation Engines as needed in your environment.	Section 12.4, “Installing Collector Managers and Correlation Engines,” on page 71.

4 Understanding License Information

The Sentinel platform comprises a broad spectrum of functionality, and different customers have different needs. NetIQ provides different licensing models to meet those needs.

Prior to Sentinel 7.3, the basic Sentinel platform was delivered as two different products; that is, Sentinel and Sentinel Log Manager. As of Sentinel 7.3, NetIQ delivers the two products as a single unitary platform to improve its delivery of new features, patches, documentation, and support, while allowing customers to select the solution capabilities that best match their needs.

The Sentinel platform provides two main solutions:

- **Sentinel Enterprise:** A full-featured solution that enables all the core real-time visual analytics functions and many additional features. Sentinel Enterprise focuses on SIEM use cases such as real-time threat detection, alerting, and remediation.
- **Sentinel for Log Management:** A solution for log management use cases such as the ability to collect, store, search, and report on data.

  Sentinel for Log Management 7.3 represents a substantial upgrade from the functionality provided in Sentinel Log Manager 1.2.2, and in some cases, significant parts of the architecture have changed. To plan your upgrade to Sentinel for Log Management 7.3, see the FAQ document available at https://www.netiq.com/products/sentinel/frequently-asked-questions/slm122-to-slm73-upgrade-faqs.html.

Depending on which solution(s) and add-ons you purchase, NetIQ will provide you with the appropriate license keys and entitlements to enable the right functionality within Sentinel. Although the license keys and entitlements govern basic access to product features and downloads, you should refer to your purchase agreement and the End-User License Agreement for additional terms and conditions.

The following table outlines the specific services and features that are enabled on each of the solutions:

Table 4-1 Sentinel Services and Features

Services and Features	Sentinel Enterprise	Sentinel for Log Management
Core Functionality ◆ Basic event collection ◆ Non-event data collection (assets, vulnerabilities, identities) ◆ Parsing and normalization ◆ Taxonomic classification of event data ◆ In-line contextual mapping ◆ Netflow collection and storage ◆ Real-time NetFlow visualization ◆ NetFlow visualization based on events ◆ Event search (local) ◆ Event reporting ◆ Event filtering ◆ Real-time event visualization ◆ Event storage ◆ Data retention policies ◆ Event store non-repudiation ◆ FIPS enablement ◆ Manually triggered actions ◆ Manual incident creation and management ◆ Incident actions and workflows ◆ iTRAC Workflows	Yes	Yes
Actions ◆ Correlation-triggered actions (only if correlation is enabled) ◆ Routing rule-triggered actions (only if rules are enabled) ◆ Manually triggered actions	Yes	Yes
Routing Rules ◆ Event routing (external) ◆ Actions triggered by routing rules (only if actions are enabled)	Yes	Yes
Sentinel Link	Yes	Yes

Services and Features	Sentinel Enterprise	Sentinel for Log Management
Correlation ◆ Real-time pattern correlation ◆ Actions triggered by correlation rules (only if actions are enabled) ◆ Alert triage ◆ Alert dashboards	Yes	No
Data Synchronization	Yes	Yes
Event data restoration from archive	Yes	Yes
Data Federation (distributed search)	Yes	Yes
Exploit Detection (Advisor)	Yes	Yes
Security Intelligence ◆ Anomaly rules ◆ Real-time statistical analysis	Yes	No

4.1 Sentinel Licenses

This section provides information about the various Sentinel licenses.

* Section 4.1.1, “Evaluation License,” on page 35
* Section 4.1.2, “Free License,” on page 36
* Section 4.1.3, “Enterprise Licenses,” on page 36

4.1.1 Evaluation License

The default evaluation license allows you to use all the features of Sentinel Enterprise for a specific evaluation period with unlimited EPS subject to the capacity of your hardware. For information about the features available in Sentinel Enterprise, see Table 4-1, “Sentinel Services and Features,” on page 34.

The expiration date of the system is based on the oldest data in the system. If you restore old events to your system, Sentinel adjusts the expiration date accordingly.

After the evaluation license expires, the system runs with a base license key that enables a limited set of features and a limited event rate of 25 EPS. The base license is also known as the free license.

After you upgrade to an enterprise license, Sentinel restores all functionality. To prevent any interruption in functionality, you must upgrade the system with an enterprise license before the evaluation license expires.

4.1.2 Free License

The free license allows you to use a limited set of features with a limited event rate of 25 EPS. The free license does not expire.

The free license allows you to collect and store events. When the EPS rate goes above 25, Sentinel stores the events received, but does not display the details of those events in the search results or reports. Sentinel tags these events with the `OverEPSLimit` tag.

The free license does not provide real-time features. You can restore all the functionality by upgrading the license to an enterprise license.

NOTE: NetIQ does not provide technical support and product updates for the free version of Sentinel.

4.1.3 Enterprise Licenses

When you purchase Sentinel, you receive a license key through the customer portal. Depending on the license you purchase, your license key enables certain features, data collection rates, and event sources. There may be additional license terms that are not enforced by the license key, therefore read your license agreement carefully.

To make changes to your licensing, contact your account manager. You can add the enterprise license key either during the installation or any time thereafter. To add the license key, see Adding a License Key in the *NetIQ Sentinel Administration Guide*.

5 Meeting System Requirements

A Sentinel implementation can vary based on the needs of your environment, so you should consult NetIQ Consulting Services or any of the NetIQ Sentinel partners prior to finalizing the Sentinel architecture.

For information about the recommended hardware, supported operating systems, appliance platforms, and browsers, see the NetIQ Sentinel Technical Information Website.

5.1 Connector and Collector System Requirements

Each Connector and Collector has its own set of system requirements and supported platforms. See the Connector and Collector documentation on the Sentinel Plug-ins Web site.

5.2 Virtual Environment

Sentinel is extensively tested and fully supported on a VMware ESX server. When you set up a virtual environment, the virtual machines must have 2 or more CPUs. To achieve comparable performance results to the physical-machine testing results on ESX or in any other virtual environment, the virtual environment should provide the same memory, CPUs, disk space, and I/O as the physical machine recommendations.

For information about physical machine recommendations, see Chapter 5, “Meeting System Requirements,” on page 37.

6 Deployment Considerations

Sentinel has a scalable architecture that can grow to handle the load you need to place on it. There are several types of load that you can place on Sentinel. This chapter provides an overview of the most important considerations to make when scaling a Sentinel deployment. A NetIQ Services or NetIQ Partner Services professional can work with you to more thoroughly design the complete system for your unique environment.

6.1 Advantages of Distributed Deployments

By default, the Sentinel server includes the following components:

- **Collector Manager:** Collector Manager provides a flexible data collection point for Sentinel. The Sentinel installer installs a Collector Manager by default during installation.
- **Correlation Engine:** Correlation Engine processes events from the real-time event stream to determine whether they should trigger any of the correlation rules.
- **NetFlow Collector Manager:** The NetFlow Collector Manager collects network flow data (NetFlow, IPFIX, and so on) from network devices such as routers, switches, and firewalls. Network flow data describes basic information about all network connections between hosts including packets and bytes transmitted, which helps you visualize the behavior of individual hosts or the entire network.

IMPORTANT: For production environments, NetIQ Corporation recommends setting up a distributed deployment because it isolates data collection components on a separate computer, which is important for handling spikes and other anomalies with maximum system stability.

This section describes the advantages of distributed deployments.

6.1.1 Advantages of Additional Collector Managers

Sentinel server includes a Collector Manager by default. However, for production environments, distributed Collector Managers provide much better isolation when large volumes of data is received. In this situation, a distributed Collector Manager may become overloaded but the Sentinel server will remain responsive to user requests.

Installing more than one Collector Manager in a distributed network provides several advantages:

- **Improved system performance:** Additional Collector Managers can parse and process event data in a distributed environment, which increases the system performance.
- **Additional data security and decreased network bandwidth requirements:** If the Collector Managers are co-located with event sources, then filtering, encryption, and data compression can be performed at the source.
- **File caching:** Additional Collector Managers can cache large amounts of data while the server is temporarily busy archiving events or processing a spike in events. This feature is an advantage for protocols such as syslog, which do not natively support event caching.

You can install additional Collector Managers at suitable locations in your network. These remote Collector Managers run Connectors and Collectors, and forward the collected data to the Sentinel server for storage and processing. For information about installing additional Collector Managers, see Section 12.4, “Installing Collector Managers and Correlation Engines,” on page 71.

NOTE: You cannot install more than one Collector Manager on a single system. You can install additional Collector Managers on remote systems, and then connect them to the Sentinel server.

6.1.2 Advantages of Additional Correlation Engines

You can deploy multiple Correlation Engines, each on its own server, without the need to replicate configurations or add databases. For environments with large numbers of Correlation rules or extremely high event rates, it can be advantageous to install more than one Correlation engine and redeploy some rules to the new Correlation engine. Multiple Correlation engines provide the ability to scale as the Sentinel system incorporates additional data sources or as event rates increase. For information on installing additional Correlation Engines, see Section 12.4, “Installing Collector Managers and Correlation Engines,” on page 71.

NOTE: You cannot install more than one Correlation Engine on a single system. You can install additional Correlation Engines on remote systems, and then connect them to the Sentinel server.

6.1.3 Advantages of Additional NetFlow Collector Managers

NetFlow Collector Manager collects network flow data from network devices. You should install additional NetFlow Collector Managers rather than using the NetFlow Collector Manager on the Sentinel server to free up system resources to other important functions such as event storage and searches.

You can install additional NetFlow Collector Managers in the following scenarios:

- In environments with many network devices and high rates of network flow data, you can install multiple NetFlow Collector Managers to distribute the load.
- If you are in a multi-tenant environment, you should install individual NetFlow Collector Manager for each tenant to collect separate network flow data per tenant.

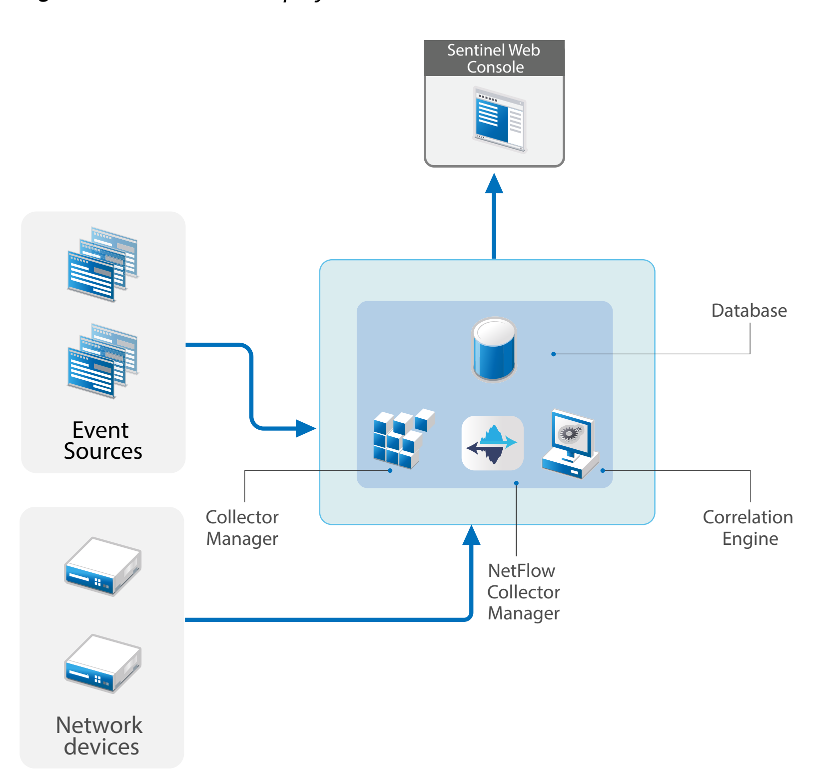
For more information about installing additional NetFlow Collector Managers, see Chapter 14, “NetFlow Collector Manager Installation,” on page 87.

6.2 All-In-One Deployment

The most basic deployment option is an all-in-one system that contains all of the Sentinel components on a single machine. All-in-one deployment is suitable only if you are putting a relatively small load on the system and do not need to monitor Windows machines. In many environments, unpredictable and fluctuating loads, and subtle resource conflicts between different components can cause performance issues.

IMPORTANT: For production environments, NetIQ Corporation recommends setting up a distributed deployment because it isolates data collection components on a separate computer, which is important for handling spikes and other anomalies with maximum system stability.

Figure 6-1 *All-In-One Deployment*



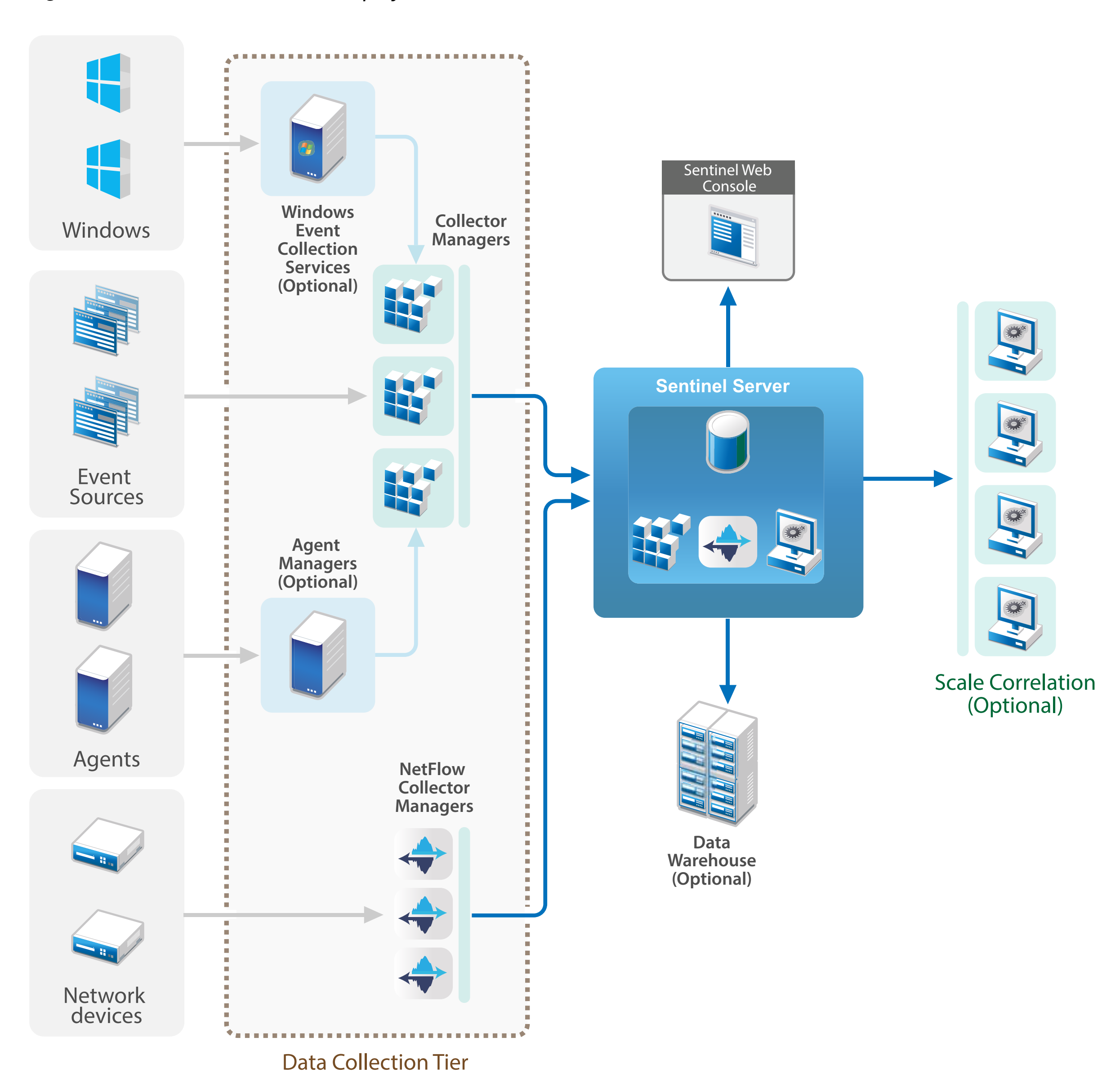
6.3 One-Tier Distributed Deployment

The one-tier deployment adds the ability to monitor Windows machines as well as handle a larger load than the all-in-one deployment. Data collection and correlation can be scaled out by adding Collector Manager, NetFlow Collector Manager, and Correlation Engine machines that off load processing from the central Sentinel server. In addition to handling the load of events, correlation rules and network flow data, remote Collector Managers, Correlation Engines, and NetFlow Collector

Managers also free up resources on the central Sentinel server to service other requests such as event storage and searches. As the load gets higher on the system, the central Sentinel server will eventually become a bottleneck and you need a deployment with more tiers to scale out further.

Optionally, you can configure Sentinel to copy event data to a data warehouse, which can be useful to offload custom reporting, analytics, and other processing to another system.

Figure 6-2 *One-Tier Distributed Deployment*



6.4 One-Tier Distributed Deployment with High Availability

The one-tier distributed deployment shows how it can be turned into a highly available system with fail-over redundancy. For more information about deploying Sentinel in High Availability, see Part VI, “Deploying Sentinel for High Availability,” on page 131.

Figure 6-3 One-Tier Distributed Deployment with High Availability

6.5 Two-Tier and Three-Tier Distributed Deployment

This deployment enables you to surpass the load handling capabilities of a single central Sentinel server and share the processing load across multiple Sentinel instance by leveraging Sentinel Link and Sentinel Distributed Search features. The data collection is load-balanced across several Sentinel servers, each having several Collector Managers, as shown in the Data Collection Tier. If you want to perform event correlation or security intelligence, you can optionally forward data up to the Analytics Tier using Sentinel Link. The Search Tier provides a convenient single access point for searching across all systems in all other tiers by using Sentinel Distributed Search. Since the search request is federated across several instances of Sentinel, this deployment also has search load-balancing properties useful in scaling to handle a heavy search load.

Network flow data is stored in the Search Tier to enable easy navigation from search results to contextual network traffic analysis.

Figure 6-4 Two-Tier and Three-Tier Distributed Deployment

6.6 Planning Partitions for Data Storage

When you install Sentinel, you must mount the disk partition for primary storage in the location where Sentinel will be installed, by default the `/var/opt/novell` directory.

The entire directory structure under the `/var/opt/novell/sentinel` directory must reside on a single disk partition to ensure proper disk usage calculations. Otherwise, the automatic data management capabilities might delete event data prematurely. For more information about the Sentinel directory structure, see Section 6.6.4, “Sentinel Directory Structure,” on page 46.

As a best practice, ensure that this data directory is located on a separate disk partition than the executables, configuration, and operating system files. The benefits of storing variable data separately include easier backup of sets of files, simpler recovery in case of corruption, and provides additional robustness if a disk partition fills up. It also improves the overall performance of systems where smaller file systems are more efficient. For more information, see “Disk Partitioning”.

6.6.1 Using Partitions in Traditional Installations

On traditional installations, you can modify the disk partition layout of the operating system prior to installing Sentinel. The administrator should create and mount the desired partitions to the appropriate directories, based on the directory structure detailed in Section 6.6.4, "Sentinel Directory Structure," on page 46. When you run the installer, Sentinel is installed into the pre-created directories resulting in an installation that spans multiple partitions.

NOTE:

- You can use the `--location` option while running the installer to specify a different top-level location than the default directories to store the file. The value that you pass to the `--location` option is prepended to the directory paths. For example, if you specify `--location=/foo`, the data directory will be `/foo/var/opt/novell/sentinel/data` and the config directory will be `/foo/etc/opt/novell/sentinel/config`.
- You must not use filesystem links (for example, soft links) for the `--location` option.

6.6.2 Using Partitions in an Appliance Installation

If you are using the DVD ISO appliance format, you can configure the partitioning of the appliance filesystem during installation by following the instructions in the YaST screens. For example, you can create a separate partition for the `/var/opt/novell/sentinel` mount point to put all data on a separate partition. However, for other appliance formats you can configure the partitioning only after installation. You can add partitions and move a directory to the new partition by using the SuSE YaST system configuration tool. For information about creating partitions after the installation, see Section 13.3.2, "Creating Partitions," on page 82.

6.6.3 Best Practices for Partition Layout

Many organizations have their own documented best-practice partition layout schemes for any installed system. The following partition proposal is intended to guide organizations without any defined policy, and considers Sentinel specific use of the filesystem. Generally, Sentinel adheres to the Filesystem Hierarchy Standard where practicable.

partition	Mount point	Size	Notes
Root	/	100GB	Contains operating system files and Sentinel binaries/configuration.
Boot	`/boot`	150MB	Boot partition
Temp	`/tmp`	30GB	Location for OS and Sentinel temporary files; isolating this on a separate partition protects application data from corruption if a runaway process fills up the temp space.

partition	Mount point	Size	Notes
Primary storage	/var/opt/novell/sentinel	Calculate using the System Sizing Information.	This area will contain the primary Sentinel collected data, plus other variable data such as log files. This partition can be shared with other systems.
Secondary storage	Location based on the type of storage, NFS, CIFS, or SAN.	Calculate using the System Sizing Information.	This is the secondary storage area, which can be mounted locally as shown or remotely.
Archival storage	Remote system	Calculate using the System Sizing Information.	This storage is for archived data.

6.6.4 Sentinel Directory Structure

By default, the Sentinel directories are in the following locations:

- The data files are in /var/opt/novell/sentinel/data and /var/opt/novell/sentinel/3rdparty directories.
- Executables and libraries are stored in the /opt/novell/sentinel directory
- Log files are in the directory /var/opt/novell/sentinel/log
- Configuration files are in the following directory /etc/opt/novell/sentinel
- The process ID (PID) file is in the directory /var/run/sentinel/server.pid

  Using the PID, administrators can identify the parent process of Sentinel server and monitor or terminate the process.

7 Deployment Considerations for FIPS140-2 Mode

Sentinel can optionally be configured to use Mozilla Network Security Services (NSS), which is a FIPS 140-2 validated cryptographic provider, for its internal encryption and other functions. The purpose of doing so is to ensure that Sentinel is ‘FIPS 140-2 Inside’ and is compliant with United States federal purchasing policies and standards.

Enabling Sentinel FIPS 140-2 mode causes communication between the Sentinel Server, Sentinel remote Collector Managers, Sentinel remote Correlation Engines, the Sentinel Web UI, the Sentinel Control Center, and the Sentinel Advisor service to use FIPS 140-2 validated cryptography.

- Section 7.1, “FIPS Implementation in Sentinel,” on page 47
- Section 7.2, “FIPS-Enabled Components in Sentinel,” on page 48
- Section 7.3, “Implementation Checklist,” on page 49
- Section 7.4, “Deployment Scenarios,” on page 49

7.1 FIPS Implementation in Sentinel

Sentinel uses the Mozilla NSS libraries that are provided by the operating system. Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) have different set of NSS packages.

The NSS cryptographic module provided by RHEL 6.3 is FIPS 140-2 validated. The NSS cryptographic module provided by SLES 11 SP3 are not yet officially FIPS 140-2 validated, but work is in progress to get the SUSE module FIPS 140-2 validated. Once the validation is available, no necessary changes to Sentinel are anticipated to provide 'FIPS 140-2 Inside' on the SUSE platform.

For more information about RHEL 6.2 FIPS 140-2 certification, see *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules*.

7.1.1 RHEL NSS Packages

Sentinel requires the following 64-bit NSS packages to support FIPS 140-2 mode:

- nspr-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

If any of these packages are not installed, you must install them before enabling FIPS 140-2 mode in Sentinel.

7.1.2 SLES NSS Packages

Sentinel requires the following 64-bit NSS packages to support FIPS 140-2 mode:

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

If any of these packages are not installed, you must install them before enabling FIPS 140-2 mode in Sentinel.

7.2 FIPS-Enabled Components in Sentinel

The following Sentinel components provide FIPS 140-2 support:

- All Sentinel platform components are updated to support FIPS 140-2 mode.
- The following Sentinel plug-ins that support cryptography are updated to support FIPS 140-2 mode:
  - Agent Manager Connector 2011.1r1 and later
  - Database (JDBC) Connector 2011.1r2 and later
  - File Connector 2011.1r1 and later - Only if the file event source type is local or NFS.
  - LDAP Integrator 2011.1r1 and later
  - Sentinel Link Connector 2011.1r3 and later
  - Sentinel Link Integrator 2011.1r2 and later
  - SMTP Integrator 2011.1r1 and later
  - Syslog Connector 2011.1r2 and later
  - Windows Event (WMI) Connector 2011.1r2 and later
  - Check Point (LEA) Connector 2011.1r2 and later

  For more information about configuring these Sentinel plug-ins to run in FIPS 140-2 mode, see "Configuring Sentinel Plug-Ins to Run in FIPS 140-2 Mode" on page 107.

The following Sentinel Connectors that support optional cryptography are not yet updated to support FIPS 140-2 mode at the time of release of this document. However, you can continue to collect events using these Connectors. For instructions on using these Connectors with Sentinel in FIPS 140-2 mode, see "Using Non-FIPS Enabled Connectors with Sentinel in FIPS 140-2 Mode" on page 113.

- Cisco SDEE Connector 2011.1r1
- File Connector 2011.1r1 - The CIFS and SCP functionalities involve cryptography and will not work in FIPS 140-2 mode.
- NetIQ Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

The following Sentinel Integrators that support SSL are not updated to support FIPS 140-2 mode at the time of release of this document. However, you may continue to use unencrypted connections when these Integrators are used with Sentinel in FIPS 140-2 mode.

- Remedy Integrator 2011.1r1 or later
- SOAP Integrator 2011.1r1 or later

Any other Sentinel plug-ins that are not listed above do not use cryptography and are not affected by enabling FIPS 140-2 mode in Sentinel. You do not need to perform any additional steps to use them with Sentinel in FIPS 140-2 mode.

For more information about the Sentinel plug-ins, see Sentinel Plug-ins Web site. If you would like to request that one of the plug-ins that has not yet been updated be made available with FIPS support, please submit a request using Bugzilla.

7.3 Implementation Checklist

The following table provides an overview of the tasks required to configure Sentinel for operation in FIPS 140-2 mode.

Tasks	For more information, see…
Plan the deployment.	Section 7.4, "Deployment Scenarios," on page 49.
Determine whether you need to enable FIPS 140-2 mode during the Sentinel installation or you want to enable it in future. To enable Sentinel in FIPS 140-2 mode during the installation, you need to select the Custom or Silent installation method during the installation process.	Section 12.2.2, "Custom Installation," on page 69. Section 12.3, "Performing a Silent Installation," on page 70 Chapter 20, "Enabling FIPS 140-2 Mode in an Existing Sentinel Installation," on page 103
Configure Sentinel Plug-ins to run in FIPS 140-2 Mode.	Section 21.5, "Configuring Sentinel Plug-Ins to Run in FIPS 140-2 Mode," on page 107.
Import certificates into the Sentinel FIPS Keystore.	Section 21.6, "Importing Certificates into FIPS Keystore Database," on page 113

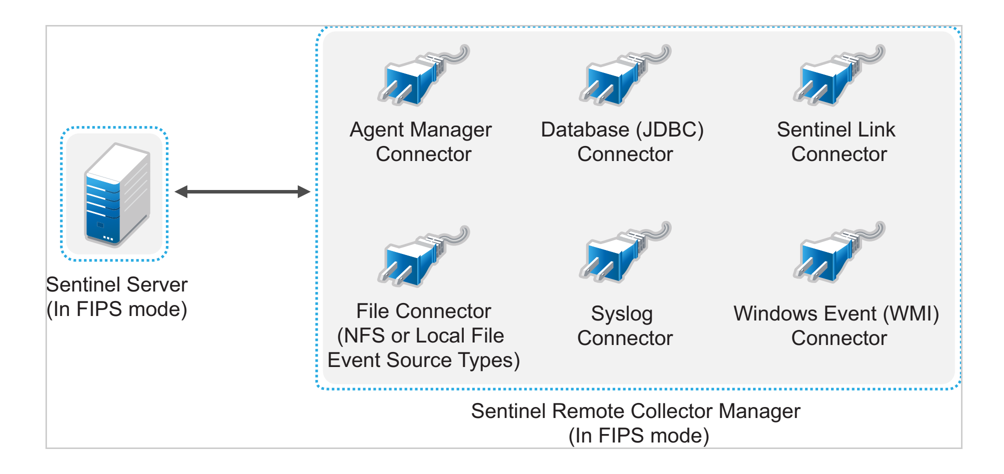
NOTE: NetIQ highly recommends taking a backup of your Sentinel systems before beginning the conversion to FIPS mode. If for some reason the server must be reverted to non-FIPS mode, the only supported method for doing so involves restoring from a backup. For more information about reverting to non-FIPS mode, see "Reverting Sentinel to Non-FIPS Mode" on page 114.

7.4 Deployment Scenarios

This section provides information about the deployment scenarios for Sentinel in FIPS 140-2 mode.

7.4.1 Scenario 1: Data Collection in Full FIPS 140-2 Mode

In this scenario, data collection is done only through the Connectors that support FIPS 140-2 mode. We assume that this environment involves a Sentinel server and data is collected through a remote Collector Manager. You may have one or more remote Collector Managers.



You must perform the following procedure only if your environment involves data collection from event sources using Connectors that support FIPS 140-2 mode.

1 You must have a Sentinel server in FIPS 140-2 mode.

> **NOTE:** If your Sentinel server (freshly installed or upgraded) is in non-FIPS mode, you must enable FIPS on Sentinel server. For more information, see “Enabling Sentinel Server to Run in FIPS 140-2 Mode” on page 103.

2 You must have a Sentinel remote Collector Manager running in FIPS 140-2 mode.

> **NOTE:** If your remote Collector Manager (freshly installed or upgraded) is running in non-FIPS mode, you must enable FIPS on the remote Collector Manager. For more information, see “Enabling FIPS 140-2 Mode on Remote Collector Managers and Correlation Engines” on page 103.

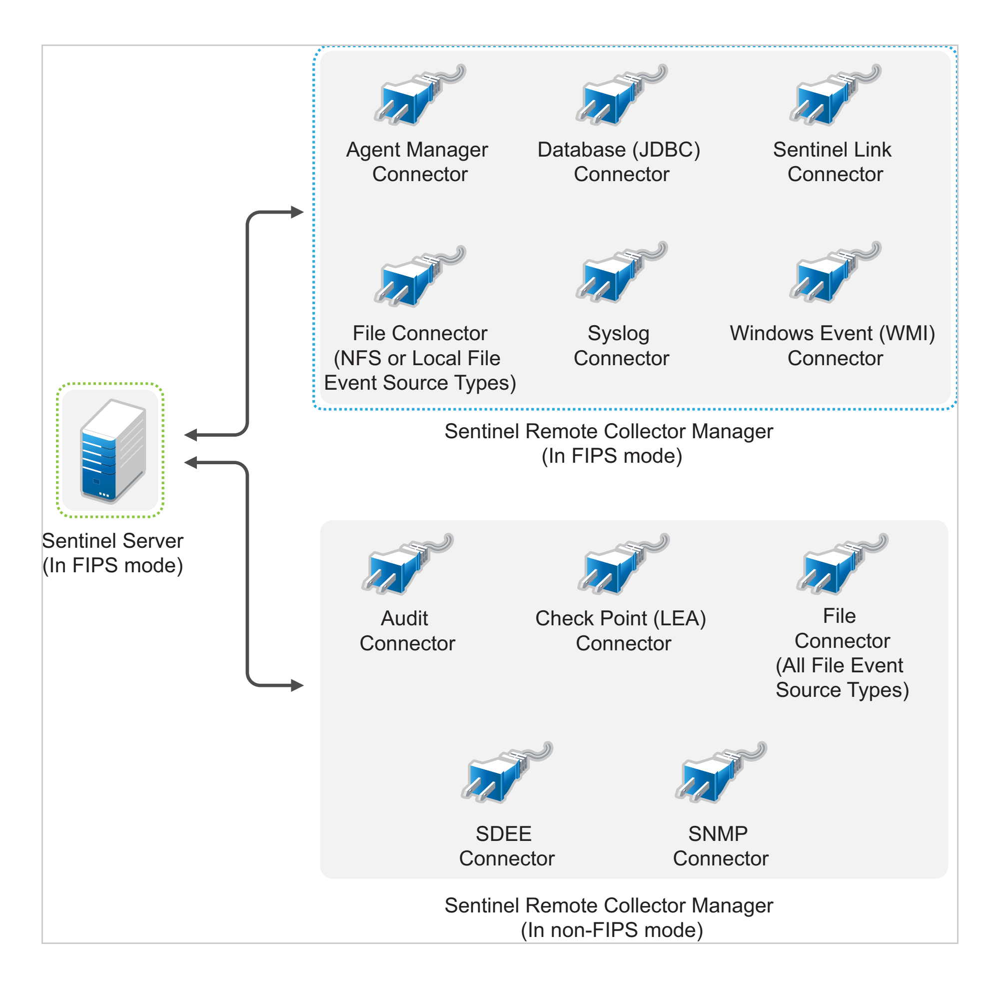
3 Ensure that FIPS server and remote Collector Managers communicates with each other.

4 Convert Remote Correlation Engines if any to run in FIPS mode. For more information, see “Enabling FIPS 140-2 Mode on Remote Collector Managers and Correlation Engines” on page 103.

5 Configure the Sentinel plug-ins to run in FIPS 140-2 mode. For more information, see “Configuring Sentinel Plug-Ins to Run in FIPS 140-2 Mode” on page 107.

7.4.2 Scenario 2: Data Collection in Partial FIPS 140-2 Mode

In this scenario, data collection is done using Connectors that support FIPS 140-2 mode and Connectors that do not support FIPS 140-2 mode. We assume that this environment involves a Sentinel server and data is collected through a remote Collector Manager. You may have one or more remote Collector Managers.



To handle data collection using Connectors that support and those that do not support the FIPS 140-2 mode, you should have two remote Collector Managers - one running in FIPS 140-2 mode for FIPS supported Connectors, and another running in non-FIPS (normal) mode for Connectors that do not support the FIPS 140-2 mode.

You must perform the following procedure if your environment involves data collection from event sources using Connectors that support FIPS 140-2 mode and Connectors that do not support FIPS 140-2 mode yet.

1 You must have a Sentinel server in FIPS 140-2 mode.

> **NOTE:** If your Sentinel server (freshly installed or upgraded) is in non-FIPS mode, you must enable FIPS on Sentinel server. For more information, see "Enabling Sentinel Server to Run in FIPS 140-2 Mode" on page 103.

2 Ensure that one remote Collector Manager is running in FIPS 140-2 mode, and another remote Collector Manager continues to run non-FIPS mode.

   2a If you do not have a FIPS 140-2 mode enabled remote Collector Manager, you must enable FIPS mode on the remote Collector Manager. For more information, see "Enabling FIPS 140-2 Mode on Remote Collector Managers and Correlation Engines" on page 103.

   2b Update the server certificate on the non-FIPS remote Collector Manager. For more information, see "Updating Server Certificates in Remote Collector Managers and Correlation Engines" on page 107.

3 Ensure that the two remote Collector Managers communicates with FIPS 140-2 enabled Sentinel server.

4 Convert Remote Correlation Engines if any to run in FIPS mode. For more information, see "Enabling FIPS 140-2 Mode on Remote Collector Managers and Correlation Engines" on page 103.

5 Configure the Sentinel plug-ins to run in FIPS 140-2 mode. For more information, see "Configuring Sentinel Plug-Ins to Run in FIPS 140-2 Mode" on page 107.

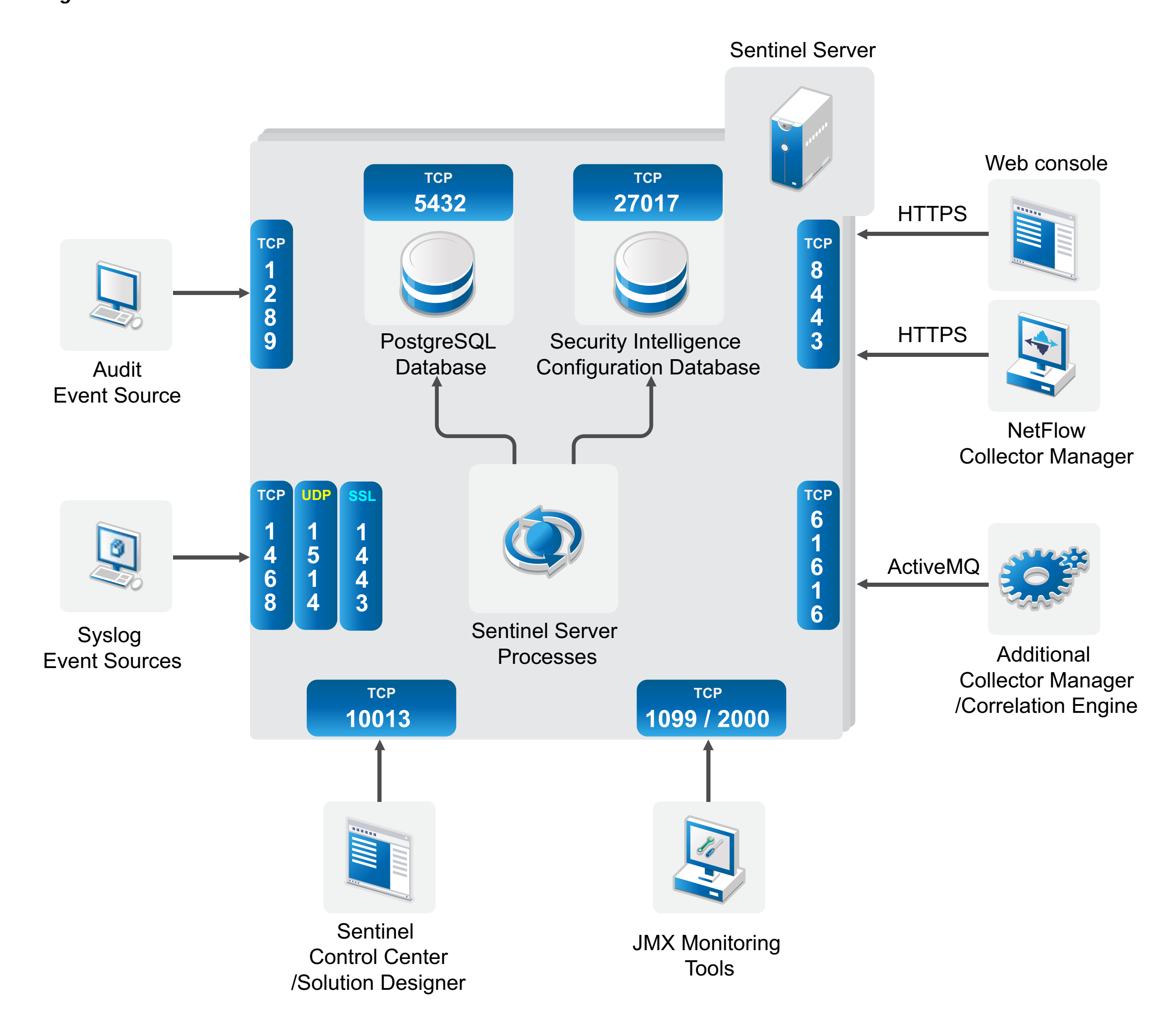
   5a Deploy Connectors that support FIPS 140-2 mode in the remote Collector Manager running in FIPS mode.

   5b Deploy the Connectors that do not support FIPS 140-2 mode in the non-FIPS remote Collector Manager.

8 Ports Used

Sentinel uses different ports for external communication with other components. For the appliance installation, the ports are opened on the firewall by default. However, for the traditional installation, you must configure the operating system on which you are installing Sentinel to open the ports on the firewall. The following figure illustrates the ports used in Sentinel:

Figure 8-1 *Ports Used in Sentinel*



8.1 Sentinel Server Ports

The Sentinel server uses the following ports for internal and external communication.

8.1.1 Local Ports

Sentinel uses the following ports for internal communication with database and other internal processes:

Ports	Description
TCP 27017	Used for the Security Intelligence configuration database.
TCP 28017	Used for the Web interface for Security Intelligence database.
TCP 32000	Used for internal communication between the wrapper process and the server process.
TCP 9200	Used for communication with alert indexing service using REST.
TCP 9300	Used for communication with alert indexing service using its native protocol.

8.1.2 Network Ports

For Sentinel to work properly, ensure that the following ports are open on the firewall:

Ports	Direction	Required/ Optional	Description
TCP 5432	Inbound	Optional. By default, this port listens only on loopback interface.	Used for the PostgreSQL database. You do not need to open this port by default. However, you must open this port when you develop reports by using the Sentinel SDK. For more information, see the Sentinel Plug-in SDK.
TCP 1099 and 2000	Inbound	Optional	Used together by monitoring tools to connect to Sentinel server process using Java Management Extensions (JMX).
TCP 1289	Inbound	Optional	Used for Audit connections.
UDP 1514	Inbound	Optional	Used for syslog messages.
TCP 8443	Inbound	Required	Used for HTTPS communication and incoming connections from NetFlow Collector Managers.
TCP 1443	Inbound	Optional	Used for SSL encrypted syslog messages.
TCP 61616	Inbound	Optional	Used for incoming connections from Collector Managers and Correlation Engines.
TCP 10013	Inbound	Required	Used by the Sentinel Control Center and Solution Designer.
TCP 1468	Inbound	Optional	Used for syslog messages.
TCP 10014	Inbound	Optional	Used by the remote Collector Managers to connect to the server through the SSL proxy. However, this is uncommon. By default, remote Collector Managers use the SSL port 61616 to connect to the server.

Ports	Direction	Required/ Optional	Description
TCP 443	Outbound	Optional	ff Advisor is used, the port initiates a connection to the Advisor service over the Internet to the Advisor Updates URL (https://secure-www.novell.com/sentinel/download/advisor/).
TCP 8443	Outbound	Optional	If distributed search is used, the port initiates a connection to other Sentinel systems to perform the distributed search.
TCP 389 or 636	Outbound	Optional	If LDAP authentication is used, the port initiates a connection to the LDAP server.
TCP/UDP 111 and TCP/UDP 2049	Outbound	Optional	If secondary storage is configured to use NFS.
TCP 137, 138, 139, 445	Outbound	Optional	If secondary storage is configured to use CIFS.
TCP JDBC (database dependent)	Outbound	Optional	If data synchronization is used, the port initiates a connection to the target database using JDBC. The port that is used is dependent on the target database.
TCP 25	Outbound	Optional	Initiates a connection to the email server.
TCP 1290	Outbound	Optional	When Sentinel forwards events to another Sentinel system, this port initiates a Sentinel Link connection to that system.
UDP 162	Outbound	Optional	When Sentinel forwards events to the system receiving SNMP traps, the port sends a packet to the receiver.
UDP 514 or TCP 1468	Outbound	Optional	This port is used when Sentinel forwards events to the system receiving Syslog messages. If the port is UDP, it sends a packet to the receiver. If the port is TCP, it initiates a connection to the receiver.

8.1.3 Sentinel Server Appliance Specific Ports

In addition to the above ports, the following ports are open for appliance.

Ports	Direction	Required/ Optional	Description
TCP 22	Inbound	Required	Used for secure shell access to the Sentinel appliance.
TCP 4984	Inbound	Required	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.
TCP 289	Inbound	Optional	Forwarded to 1289 for Audit connections.
TCP 443	Inbound	Optional	Forwarded to 8443 for HTTPS communication.
UDP 514	Inbound	Optional	Forwarded to 1514 for syslog messages.
TCP 1290	Inbound	Optional	Sentinel Link port that is allowed to connect through the SuSE Firewall.

Ports	Direction	Required/ Optional	Description
UDP and TCP 40000 - 41000	Inbound	Optional	Ports that can be used when configuring data collection servers, such as syslog. Sentinel does not listen on these ports by default.
TCP 443 or 80	Outbound	Required	Initiates a connect to the NetIQ appliance software update repository on the Internet or a Subscription Management Tool service in your network.
TCP 80	Outbound	Optional	Initiates a connection to the Subscription Management Tool.

8.2 Collector Manager Ports

The Collector Manager uses the following ports to communicate with other components.

8.2.1 Network Ports

For Sentinel Collector Manager to work properly, ensure that the following ports are open on the firewall:

Ports	Direction	Required/ Optional	Description
TCP 1289	Inbound	Optional	Used for Audit connections.
UDP 1514	Inbound	Optional	Used for syslog messages.
TCP 1443	Inbound	Optional	Used for SSL encrypted syslog messages.
TCP 1468	Inbound	Optional	Used for syslog messages.
TCP 1099 and 2000	Inbound	Optional	Used together by monitoring tools to connect to Sentinel server process using Java Management Extensions (JMX).
TCP 61616	Outbound	Required	Initiates a connection to the Sentinel server.

8.2.2 Collector Manager Appliance Specific Ports

In addition to the above ports, the following ports are open for the Sentinel Collector Manager appliance.

Ports	Direction	Required/ Optional	Description
TCP 22	Inbound	Required	Used for secure shell access to the Sentinel appliance.
TCP 4984	Inbound	Required	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.
TCP 289	Inbound	Optional	Forwarded to 1289 for Audit connections.
UDP 514	Inbound	Optional	Forwarded to 1514 for syslog messages.

Ports	Direction	Required/ Optional	Description
TCP 1290	Inbound	Optional	This is the Sentinel Link port that is allowed to connect through the SuSE Firewall.
UDP and TCP 40000 - 41000	Inbound	Optional	Ports that can be used when configuring data collection servers, such as syslog. Sentinel does not listen on these ports by default.
TCP 443	Outbound	Required	Initiates a connection to the NetIQ appliance software update repository on the Internet or a Subscription Management Tool service in your network.
TCP 80	Outbound	Optional	Initiates a connection to the Subscription Management Tool.

8.3 Correlation Engine Ports

The Correlation Engine uses the following ports to communicate with other components.

8.3.1 Network Ports

For Sentinel Correlation Engine to work properly, ensure that the following ports are open on the firewall:

Ports	Direction	Required/Optional	Description
TCP 1099 and 2000	Inbound	Optional	Used together by monitoring tools to connect to Sentinel server process using Java Management Extensions (JMX).
TCP 61616	Outbound	Required	Initiates a connection to the Sentinel server.

8.3.2 Correlation Engine Appliance Specific Ports

In addition to the above ports, the following ports are open on Sentinel Correlation Engine appliance.

Ports	Direction	Required/ Optional	Description
TCP 22	Inbound	Required	Used for secure shell access to the Sentinel appliance.
TCP 4984	Inbound	Required	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.
TCP 443	Outbound	Required	Initiates a connection to the NetIQ appliance software update repository on the Internet or a Subscription Management Tool service in your network.
TCP 80	Outbound	Optional	Initiates a connection to the Subscription Management Tool.

8.4 NetFlow Collector Manager Ports

The NetFlow Collector Manager uses the following ports to communicate with other components:

Ports	Direction	Required/ Optional	Description
HTTPS 8443	Outbound	Required	Initiates a connection to the Sentinel server.
3578	Inbound	Required	Used for receiving network flow data from network devices.

9 Installation Options

You can perform a traditional installation of Sentinel or install the appliance. This chapter provides information about the two installation options.

9.1 Traditional Installation

The traditional installation installs Sentinel on an existing operating system, by using the application installer. You can install Sentinel in the following ways:

- **Interactive:** The installation proceeds with user inputs. During installation, you can record the installation options (user inputs or default values) to a file, which you can use later for silent installation.You can either perform a standard installation or a custom installation.

Standard Installation	Custom Installation
Uses the default values for the configuration. User input is required only for the password.	Prompts you to specify the values for the configuration setup. You can either select the default values or specify the necessary values.
Installs with default evaluation key.	Allows you to install with the default evaluation license key or with a valid license key.
Allows you to specify the admin password and uses the admin password as the default password for both dbauser and appuser.	Allows you to specify the admin password. For dbauser and appuser, you can either specify new password or use admin password.
Installs the default ports for all the components.	Allows you to specify ports for different components.
Installs Sentinel in non-FIPS mode.	Allows you to install Sentinel in FIPS 140-2 mode.
Authenticates users with the internal database.	Provides the option set up LDAP authentication for Sentinel in addition to the database authentication. When you configure Sentinel for LDAP authentication, users can log in to the server by using their Novell eDirectory or Microsoft Active Directory credentials.

  For more information about interactive installation, see Section 12.2, “Performing Interactive Installation,” on page 67.

- **Silent:** If you want to install multiple Sentinel servers in your deployment, you can record the installation options during the standard or custom installation in a configuration file and then use the file to run an unattended installation. For more information on silent installation, see **Section 12.3, “Performing a Silent Installation,” on page 70**.

9.2 Appliance Installation

The appliance installation installs both the SLES 11 SP3 64-bit operating system and Sentinel.

The Sentinel appliance is available in the following formats:

- An OVF appliance image
- A hardware appliance Live DVD image that is directly deployable to a hardware server

For more information on appliance installation, see Chapter 13, “Appliance Installation,” on page 77.

III Installing Sentinel

This section provides information about installing Sentinel and additional components.

10 Installation Overview

The Sentinel installation installs the following components in the Sentinel server:

- **Sentinel server process:** This is the primary component of Sentinel. The Sentinel server process processes requests from other components of Sentinel and enables seamless functionality of the system.The Sentinel server process handles requests, such as filtering data, processing search queries, and managing administrative tasks that include user authentication and authorization.
- **Web server:** Sentinel uses Jetty as its Web server to allow secure connection to the Sentinel Web interface.
- **PostgreSQL database:** Sentinel has a built-in database that stores Sentinel configuration information, asset and vulnerability data, identity information, incident and workflow status, and so on.
- **MongoDB database:** Stores the Security Intelligence data.
- **Collector Manager:** Collector Manager provides a flexible data collection point for Sentinel. The Sentinel installer installs a Collector Manager by default during installation.
- **NetFlow Collector Manager:** The NetFlow Collector Manager collects network flow data (NetFlow, IPFIX, and so on) from network devices such as routers, switches, and firewalls. Network flow data describes basic information about all network connections between hosts including packets and bytes transmitted, which helps you visualize the behavior of individual hosts or the entire network.
- **Correlation Engine:** Correlation Engine processes events from the real-time event stream to determine whether they should trigger any of the correlation rules.
- **Advisor:** Advisor, powered by Security Nexus, is an optional data subscription service that provides device-level correlation between real-time events, from intrusion detection and prevention systems, and from enterprise vulnerability scan results. For more information about Advisor, see “Detecting Vulnerabilities and Exploits”in the *NetIQ Sentinel Administration Guide*.
- **Sentinel plug-ins:** Sentinel supports a variety of plug-ins to expand and enhance system functionality. Some of these plug-ins are preinstalled. You can download additional plug-ins and updates from the Sentinel Plug-ins Web site. Sentinel plug-ins include the following:
  - Collectors
  - Connectors
  - Correlation rules and actions
  - Reports
  - iTRAC workflows
  - Solution packs

Sentinel has a highly scalable architecture, and if high event rates are expected, you can distribute components across several machines to achieve the best performance for the system. For production environments, NetIQ Corporation recommends setting up a distributed deployment because it isolates data collection components on a separate machine, which is important for handling spikes and other anomalies with maximum system stability. For more information, see Section 6.1, “Advantages of Distributed Deployments,” on page 39.

11 Installation Checklist

Ensure that you have completed the following tasks before you start the installation:

- ❒ Verify that your hardware and software meet the system requirements listed in Chapter 5, “Meeting System Requirements,” on page 37.
- ❒ If there was a previous installation of Sentinel, ensure that there are no files or system settings remaining from a previous installation. For more information, see Appendix B, “Uninstalling,” on page 163.
- ❒ If you plan to install the licensed version, obtain your license key from the NetIQ Customer Care Center.
- ❒ Ensure that the ports listed in Chapter 8, “Ports Used,” on page 53 are opened in the firewall.
- ❒ For the Sentinel installer to work properly, the system must be able to return the hostname or a valid IP address. To do this, add the hostname to the `/etc/hosts` file to the line containing the IP address, then enter `hostname -f` to make sure that the hostname is displayed properly.
- ❒ Synchronize time by using the Network Time Protocol (NTP).
- ❒ **On RHEL systems:** For optimal performance, the memory settings must be set appropriately for the PostgreSQL database. The SHMMAX parameter must be greater than or equal to 1073741824.

  To set the appropriate value, append the following information in the `/etc/sysctl.conf` file:

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```
- ❒ **For traditional installations:**

  The operating system for the Sentinel server must include at least the Base Server components of the SLES server or the RHEL 6 server. Sentinel requires the 64-bit versions of the following RPMs:

  - bash
  - bc
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

12 Traditional Installation

This chapter provides information about the various ways to install Sentinel.

12.1 Understanding Installation Options

`./install-sentinel --help` displays the following options:

Options	Value	Description
--location	Directory	Specifies a directory other than the root (/) to install Sentinel.
-m, --manifest	File name	Specifies a product manifest file to use instead of the default manifest file.
--no-configure		Specifies to not configure the product after installation.
-n, --no-start		Specifies to not start or restart Sentinel after installation or configuration.
-r, --recordunattended	Filename	Specifies a file to record the parameters that can be used for unattended installation.
-u, --unattended	Filename	Uses the parameters from the specified file in order to install Sentinel on unattended systems.
-h, --help		Displays the options that can be used while installing Sentinel.
-l, --log-file	Filename	Records log messages to a file.
--no-banner		Suppresses the display of banner message.
-q, --quiet		Displays fewer messages.
-v, --verbose		Displays all messages during installation.

12.2 Performing Interactive Installation

This section provides information about standard and custom installation.

12.2.1 Standard Installation

Use the following steps to perform a standard installation:

1 Download the Sentinel installation file from the NetIQ Downloads Web site:

  1a In the **Product or Technology** field, browse to and select **SIEM-Sentinel**.

  1b Click **Search**.

  1c Click the button in the **Download** column for **Sentinel Evaluation**.

  1d Click **proceed to download**, then specify your customer name and password.

  1e Click **download** for the installation version for your platform.

2 Specify at the command line the following command to extract the installation file.

```
tar zxvf <install_filename>
```

Replace <*install_filename*> with the actual name of the install file.

3 Change to the directory where you extracted the installer:

```
cd <directory_name>
```

4 Specify the following command to install Sentinel:

```
./install-sentinel
```

or

If you want to install Sentinel on more than one system, you can record your installation options in a file. You can use this file for an unattended Sentinel installation on other systems. To record your installation options, specify the following command:

```
./install-sentinel -r <response_filename>
```

5 Specify the number for the language you want to use for the installation, then press Enter.

The end user license agreement is displayed in the selected language.

6 Press the Spacebar to read through the license agreement.

7 Enter `yes` or `y` to accept the license and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt for the configuration type.

8 When prompted, specify `1` to proceed with the standard configuration.

Installation proceeds with the default evaluation license key included with the installer. At any time during or after the evaluation period, you can replace the evaluation license with a license key you have purchased.

9 Specify the password for the administrator user `admin`.

10 Confirm the password again.

This password is used by `admin`, `dbauser`, and `appuser`.

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

12.2.2 Custom Installation

If you are installing Sentinel with a custom configuration, you can specify the license key, change the password for different users, and specify values for different ports that are used to interact with the internal components.

1 Download the Sentinel installation file from the NetIQ Downloads Web site:

1a In the **Product or Technology** field, browse to and select **SIEM-Sentinel**.

1b Click **Search**.

1c Click the button in the **Download** column for **Sentinel 7.2 Evaluation**.

1d Click **proceed to download**, then specify your customer name and password.

1e Click **download** for the installation version for your platform.

2 Specify at the command line the following command to extract the installation file.

```
tar zxvf <install_filename>
```

Replace *<install_filename>* with the actual name of the install file.

3 Specify the following command in the root of the extracted directory to install Sentinel:

```
./install-sentinel
```

or

If you want to use this custom configuration to install Sentinel on more than one system, you can record your installation options in a file. You can use this file for an unattended Sentinel installation on other systems. To record your installation options, specify the following command:

```
./install-sentinel -r <response_filename>
```

4 Specify the number for the language you want to use for the installation, then press Enter.

The end user license agreement is displayed in the selected language.

5 Press the Spacebar to read through the license agreement.

6 Enter `yes` or `y` to accept the license agreement and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt for the configuration type.

7 Specify `2` to perform a custom configuration of Sentinel.

8 Enter `1` to use the default evaluation license key

or

Enter `2` to enter a purchased license key for Sentinel.

9 Specify the password for the administrator user `admin` and confirm the password again.

10 Specify the password for the database user `dbauser` and confirm the password again.

The `dbauser` account is the identity used by Sentinel to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.

11 Specify the password for the application user `appuser` and confirm the password again.

12 Change the port assignments for the Sentinel services by entering the desired number, then specifying the new port number.

13 After you have changed the ports, specify 7 for done.

14 Enter `1` to authenticate users using only the internal database.

or

If you have configured an LDAP directory in your domain, enter 2 to authenticate users by using LDAP directory authentication.

The default value is 1.

15 ***If you want to enable Sentinel in FIPS 140-2 mode***, press y.

15a Specify a strong password for the keystore database and confirm the password again.

NOTE: The password must be at least seven characters long. The password must contain at least three of the following character classes: Digits, ASCII lowercase letters, ASCII uppercase letters, ASCII non-alphanumeric characters, and non-ASCII characters.

If an ASCII uppercase letter is the first character or a digit is the last character, they are not counted.

15b If you want to insert external certificates into the keystore database to establish trust, press y and specify the path for the certificate file. Otherwise, press n

15c Complete the FIPS 140-2 mode configuration by following the tasks mentioned in Chapter 21, “Operating Sentinel in FIPS 140-2 Mode,” on page 105.

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

12.3 Performing a Silent Installation

The silent or unattended installation is useful if you need to install more than one Sentinel server in your deployment. In such a scenario, you can record the installation parameters during the interactive installation and then run the recorded file on other servers. You can record the installation parameters while installing Sentinel with the standard configuration or a custom configuration.

To perform silent installation, ensure that you have recorded the installation parameters to a file. For information on creating the response file, see Section 12.2.1, “Standard Installation,” on page 68 or Section 12.2.2, “Custom Installation,” on page 69.

To enable Sentinel in FIPS 140-2 mode, ensure that the response file includes the following parameters:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

To perform a silent installation, use the following steps:

1. Download the installation files from the NetIQ Downloads Web site.
2. Log in as root to the server where you want to install Sentinel.
3. Specify the following command to extract the install files from the tar file:

   ```
   tar -zxvf <install_filename>
   ```

   Replace <*install_filename*> with the actual name of the install file.

4 Specify the following command to install Sentinel in silent mode:

```
./install-sentinel -u <response_file>
```

The installation proceeds with the values stored in the response file.

5 **(Conditional) If you chose to enable FIPS 140-2 mode,** complete the FIPS 140-2 mode configuration by following the tasks mentioned in Chapter 21, "Operating Sentinel in FIPS 140-2 Mode," on page 105.

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

12.4 Installing Collector Managers and Correlation Engines

By default, Sentinel installs a Collector Manager and a Correlation Engine. For production environments, NetIQ Corporation recommends setting up a distributed deployment because it isolates data collection components on a separate machine, which is important for handling spikes and other anomalies with maximum system stability. For information about the advantages of installing additional components, see Section 6.1, "Advantages of Distributed Deployments," on page 39.

IMPORTANT: You must install the additional Collector Manager or the Correlation Engine on separate systems. The Collector Manager or the Correlation Engine must not be on the same system where the Sentinel server is installed.

12.4.1 Installation Checklist

Ensure that you have completed the following tasks before starting the installation.

- ❒ Make sure that your hardware and software meet the minimum requirements. For more information, see Chapter 5, "Meeting System Requirements," on page 37.
- ❒ Synchronize time by using the Network Time Protocol (NTP).
- ❒ A Collector Manager requires network connectivity to the message bus port (61616) on the Sentinel server. Before you start installing the Collector Manager, make sure that all firewall and network settings are allowed to communicate over this port.

12.4.2 Installing Collector Managers and Correlation Engines

1 Launch the Sentinel Web interface by specifying the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The *<IP_Address_Sentinel_server>* is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

Log in with the username and password specified during the installation of the Sentinel server.

2. In the toolbar, click **Downloads**.
3. Click **Download Installer** under the required installation.
4. Click **Save File** to save the installer to the desired location.
5. Specify the following command to extract the installation file.

```
tar zxvf <install_filename>
```

Replace <*install_filename*> with the actual name of the install file.

6. Change to the directory where you extracted the installer.
7. Specify the following command to install the Collector Manager or the Correlation Engine:

For Collector Manager:

```
./install-cm
```

For Correlation Engine:

```
./install-ce
```

8. Specify the number for the language you want to use for the installation.

The end user license agreement is displayed in the selected language.

9. Press the Spacebar to read through the license agreement.
10. Enter `yes` or `y` to accept the license agreement and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt for the configuration type.

11. When prompted, specify 1 to proceed with the standard configuration.
12. Enter default Communication Server Hostname or IP Address of the machine on which Sentinel is installed.

The Sentinel server certificate is displayed.

13. Specify the ActiveMQ user credentials for the Collector Manager or the Correlation Engine.

The ActiveMQ user credentials are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located in the Sentinel server.

14. When prompted to accept the certificate, verify the certificate using the following command:

```
/opt/novell/sentinel/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

Compare the certificate output with the Sentinel server certificate displayed in Step 12.

15. Accept the certificate if the certificate output matches the Sentinel server certificate.
16. Enter `yes` or `y` to enable FIPS 140-2 mode in Sentinel and continue with the FIPS configuration.
17. Continue with the installation as prompted until the installation is complete.

12.4.3 Adding a Custom ActiveMQ User for the Collector Manager or Correlation Engine

Sentinel recommends that you use the default ActiveMQ usernames for the remote Collector Manager and Correlation Engine. However, if you have installed multiple remote Collector Managers and you want to identify them separately, you can create new ActiveMQ users:

1 Log in to the server as the Sentinel user who has access to the installation files.

2 Open the `activemqgroups.properties` file.

   This file is located in the `/<install_dir>/etc/opt/novell/sentinel/config/` directory.

3 Add the new ActiveMQ usernames separated by comma as follows:

   For Collector Manager, add the new users in the cm section. For example:

   ```
   cm=collectormanager,cmuser1,cmuser2,...
   ```

   For Correlation Engine, add the new users in the admins section. For example:

   ```
   admins=system,correlationengine,ceuser1,ceuser2,...
   ```

4 Save and close the file.

5 Open the `activemqusers.properties` file.

   This file is located in the `/<install_dir>/etc/opt/novell/sentinel/config/` directory.

6 Add the password for the ActiveMQ user you created in Step 3.

   The password can be any random string. For example:

   For Collector Manager users:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   collectormanager=1c51ae56
   cmuser1=1b51de55
   cmuser2=1a51ce57
   ```

   For Correlation Engine users:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```

7 Save and close the file.

8 Restart the Sentinel server.

12.5 Installing Sentinel as a Non-root User

If your organizational policy does not allow you to run the full installation of Sentinel as `root`, you can install Sentinel as a `non-root` user; that is, as the `novell` user. In this installation, a few steps are performed as a `root` user, then you proceed to install Sentinel as the `novell` user created by the `root` user. Finally, the `root` user completes the installation.

When installing Sentinel as a `non-root` user, you should install Sentinel as the novell user. NetIQ Corporation does not support non-root installations other than the novell user, although the installation proceeds successfully.

1 Download the installation files from the NetIQ Downloads Web site.

2 Specify the following command at the command line to extract the install files from the tar file:

```
tar -zxvf <install_filename>
```

Replace *<install_filename>* with the actual name of the install file.

3. Log in as `root` to the server where you want to install Sentinel as `root`.
4. Specify the following command:

```
./bin/root_install_prepare
```

A list of commands to be executed with root privileges is displayed. If you want the non-root user to install Sentinel in non-default location, specify the --location option along with the command. For example:

```
./bin/root_install_prepare --location=/foo
```

The value that you pass to the `--location` option `foo` is prepended to the directory paths.

This also creates a `novell` group and a `novell` user, if they do not already exist.

5. Accept the command list.

The displayed commands are executed.

6. Specify the following command to change to the newly created non-root user; that is, `novell`:

```
su novell
```

7. (Conditional) To do an interactive installation:

7a Specify the appropriate command depending on the component you are installing:

Component	Command
Sentinel server	**Default location:** `./install-sentinel`
	Non-default location: `./install-sentinel --location=/foo`
Collector Manager	**Default location:** `./install-cm`
	Non-default location: `./install-cm --location=/foo`
Correlation Engine	**Default location:** `./install-ce`
	Non-default location: `./install-cm --location=/foo`
NetFlow Collector Manager	**Default location:** `./install-netflow`
	Non-default location: `./install-netflow --location=/foo`

7b Continue with Step 9.

8. (Conditional) To perform silent installation, ensure that you have recorded the installation parameters to a file. For information on creating the response file, see Section 12.2.1, “Standard Installation,” on page 68 or Section 12.2.2, “Custom Installation,” on page 69.

To do a silent installation:

8a Specify the appropriate command depending on the component you are installing:

Component	Command
Sentinel server	**Default location:** ./install-sentinel -u <*response_file*> **Non-default location:** ./install-sentinel --location=/foo -u <*response_file*>
Collector Manager	**Default location:** ./install-cm -u <*response_file*> **Non-default location:** ./install-cm --location=/foo -u <*response_file*>
Correlation Engine	**Default location:** ./install-ce -u <*response_file*> **Non-default location:** ./install-ce --location=/foo -u <*response_file*>
NetFlow Collector Manager	**Default location:** ./install-netflow -u <*response_file*> **Non-default location:** ./install-netflow --location=/foo -u <*response_file*>

The installation proceeds with the values stored in the response file.

8b Continue with Step 12.

9 Specify the number for the language you want to use for the installation.

The end user license agreement is displayed in the selected language.

10 Read the end user license and enter yes or y to accept the license and continue with the installation.

The installation starts installing all RPM packages. This installation might take a few seconds to complete.

11 You are prompted to specify the mode of installation.

- If you select to proceed with the standard configuration, continue with Step 8 through Step 10 in Section 12.2.1, “Standard Installation,” on page 68.
- If you select to proceed with the custom configuration, continue with Step 7 through Step 14 in Section 12.2.2, “Custom Installation,” on page 69.

12 Log in as a root user and specify the following command to finish installation:

```
./bin/root_install_finish
```

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The *<IP_Address_Sentinel_server>* is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

13 Appliance Installation

The Sentinel appliance is a ready-to-run software appliance built on SUSE Studio. The appliance combines a hardened SLES operating system and the Sentinel software integrated update service to provide an easy and seamless user experience that allows customers to leverage existing investments. Before you install the Sentinel appliance, review new functionality and known issues in the supported SLES Release Notes.

The Sentinel appliance image is packaged in both ISO and OVF formats that can be deployed to the virtual environments. For information about supported virtualization platforms, see the NetIQ Sentinel Technical Information Website.

13.1 Installing the Sentinel ISO Appliance

This section provides information about installing Sentinel, Collector Managers, and Correlation Engines using the ISO appliance image. This image format allows you to generate a full disk image format that can be deployed directly to hardware, either physical (bare metal) or virtual (uninstalled virtual machine in a hypervisor) by using a bootable ISO DVD image.

13.1.1 Prerequisites

Ensure that the environment where you are going to install Sentinel as ISO appliance meets the following prerequisites:

- (Conditional) If you are installing Sentinel ISO appliance on bare metal hardware, download the appliance ISO disk image from the support site, unpack the file, and make a DVD.
- Ensure that the system where you want to install the ISO disk image has a minimum memory of 4.5 GB for the installation to complete.
- Ensure that the minimum hard disk space is 50 GB for the installer to make the automatic partition proposal.

13.1.2 Installing Sentinel

To install the Sentinel ISO appliance:

1 Download the ISO virtual appliance image from the NetIQ Download Website.

2 (Conditional) If you are using a hypervisor:

Set up the virtual machine using the ISO virtual appliance image, and power it on.

or

Copy the ISO image into a DVD, set up the virtual machine using the DVD, and power it on.

3 (Conditional) If you are installing the Sentinel appliance on bare metal hardware:

   3a Boot the physical machine from the DVD drive with the DVD.

   3b Follow the installation wizard on-screen instructions.

   3c Run the Live DVD appliance image by selecting the top entry in the boot menu.

   The installation first checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation is automatically terminated. If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. Enter y if you want to continue with the installation, or enter n if you do not want to proceed.

4 Select the language of your choice, then click **Next**.

5 Select the keyboard Configuration, then click **Next**.

6 Read and accept the SUSE Enterprise Server Software License Agreement. Click **Next**

7 Read and accept the NetIQ Sentinel End User License Agreement. Click **Next**

8 On the Hostname and Domain Name page, specify the hostname and domain name. Deselect **Assign Hostname to Loopback IP**.

9 Click **Next**.

10 Choose one of the following connection settings options:

   - To use the current network connection settings, select **Use the following configuration** on the Network Configuration II page.
   - To change the network connection settings, click **Change**, then make the desired changes.

11 Click **Next**.

12 Set the Time and Date, then click **Next**.

   To change the NTP configuration after installation, use YaST from the appliance command line. You can use WebYast to change the time and date settings, but not the NTP configuration.

   If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

13 Set the `root` password, then click **Next**.

14 Set the Sentinel admin password, then click **Next**.

   Ensure that **Install Sentinel appliance to hard drive (for Live DVD image only)** is selected to install the appliance on the physical server. This check box is selected by default.

   If you deselect this check box, the appliance is not installed on the physical server and will run only in the LIVE DVD mode, proceed to Step 21.

15 In the YaST2 live installer console, select **Next**.

   The YaST2 live installer console installs the appliance to the hard disk. The YaST2 live installer console repeats some of the earlier installation steps.

16 The **Suggested Partitioning** screen displays the recommended partition setup. Review the partition setup, configure the setup (if necessary), and then select **Next**. Modify these settings only if you are familiar with configuring partitions in SLES.

You can configure the partition setup by using the various partitioning options on the screen. For more information about configuring partitions, see Using the YaST Partitioner in the *SLES documentation* and Section 6.6, “Planning Partitions for Data Storage,” on page 44.

17 Enter the root password and select **Next**.

18 The **Live Installation Settings** screen displays the selected installation settings. Review the settings, configure the settings (if necessary), and then select **Install**.

19 Select **Install** to confirm the Installation.

Wait until the installation finishes. It might take few minutes for all services to start up after installation because the system performs a one-time initialization.

20 Select **OK** to reboot the system.

21 Make a note of the appliance IP address that is shown in the console.

22 Enter the root username and password at the console to log in to the appliance.

The default value for the username is `root` and the password is the password you set in Step 17.

23 Proceed with Section 13.3, “Post-Installation Configuration for the Appliance,” on page 82.

13.1.3 Installing Collector Managers and Correlation Engines

The procedure to install a Collector Manager or a Correlation Engine is the same except that you need to download the appropriate ISO appliance file from the NetIQ Download website.

1 Complete Step 1 through Step 13 in Section 13.1.2, “Installing Sentinel,” on page 77.

2 Specify the following configuration for the Collector Manager or the Correlation Engine:

- **Sentinel Server Hostname or IP Address:** Specify the host name or IP address of the Sentinel server that the Collector Manager or Correlation Engine should connect to.
- **Sentinel Communication Channel Port:** Specify the Sentinel server communication channel port number. The default port number is `61616`.
- **Communication Channel User Name:** Specify the communication channel user name, which is the Collector Manager or Correlation Engine user name.
- **Communication Channel User Password:** Specify the communication channel user Password.

  The communication channel user credentials are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.

  To verify the credentials, see the following line in the `activemqusers.properties` file:

  For Collector Manager:

  ```
  collectormanager=<password>
  ```

  In this example, `collectormanager` is the username and the corresponding value is the password.

  For Correlation Engine:

  ```
  correlationengine=<password>
  ```

  In this example, `correlationengine` is the username and the corresponding value is the password.

- **Install Sentinel appliance to hard drive (for Live DVD image only):** Ensure you select this check box to install the appliance on the physical server.

  If you deselect this check box, the appliance will not be installed on the physical server and will run only in the Live DVD mode.

3 Click **Next**.
4 Accept the certificate when prompted.
5 Complete Step 15 through Step 20 in Section 13.1.2, “Installing Sentinel,” on page 77.
6 Make a note of the appliance IP address that is shown in the console.

  The console displays a message that this appliance is the Sentinel Collector Manager or Correlation Engine depending on what you chose to install, along with the IP address. The Console also displays the Sentinel server user interface IP address.
7 Complete Step 22 through Step 23 in Section 13.1.2, “Installing Sentinel,” on page 77.

13.2 Installing the Sentinel OVF Appliance

This section provides information about installing Sentinel, Collector Manager, and Correlation Engine as an OVF appliance image.

The OVF format is a standard virtual machine format that is supported by most hypervisors, either directly or by a simple conversion. Sentinel supports OVF appliance with two certified hypervisors, but you can also use it with other hypervisors.

13.2.1 Installing Sentinel

To install the Sentinel OVF appliance:

1 Download the OVF virtual appliance image from the NetIQ Download Website.
2 In your hypervisor's management console, import the OVF image file as a new virtual machine. Allow the hypervisor to convert the OVF image into the native format if you are prompted to do so.
3 Review the virtual hardware resources allocated to your new virtual machine to ensure that they meet the Sentinel requirements.
4 Power on the virtual machine.
5 Select the language of your choice, then click **Next**.
6 Select the keyboard layout, then click **Next**.
7 Read and accept the SUSE Linux Enterprise Server (SLES) 11 SP3 Software License Agreement.
8 Read and accept the NetIQ Sentinel End User License Agreement.
9 On the Hostname and Domain Name page, specify the hostname and domain name. Deselect **Assign Hostname to Loopback IP**.
10 Click **Next**. The hostname configurations are saved.

11 Choose one of the following network connection options:

- To use the current network connection settings, select **Use Following Configuration** on the Network Configuration II page, then click **Next**.
- To change the network connection settings, select **Change**, make the desired changes, then click **Next**.

The network connection settings are saved.

12 Set the time and date, then click **Next**.

To change the NTP configuration after installation, use YaST from the appliance command line. You can use WebYast to change the time and date, but not the NTP configuration.

If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

13 Set the `root` password, then click **Next**.

The installation checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation will not let you proceed and the **Next** button is greyed out.

If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. When this message is displayed, click **Next** to continue with the installation.

14 Set the Sentinel admin password, then click **Next**.

It might take a few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

15 Make a note of the appliance IP address that is shown in the console. Use the same IP address to access the Sentinel Web Console.

13.2.2 Installing Collector Managers and Correlation Engines

To install a Collector Manager or a Correlation Engine on a VMware ESX server as an OVF appliance image:

1 Complete Step 1 through Step 10 in Section 13.2.1, “Installing Sentinel,” on page 80.

2 Specify the host name/IP address of the Sentinel server that the Collector Manager should connect to.

3 Specify the Communication Server port number. The default port is `61616`.

4 Specify the ActiveMQ user name, which is the Collector Manager or Correlation Engine username. The default username is `collectormanager` for Collector Manager and `correlationengine` for Correlation Engine.

5 Specify the password for the ActiveMQ user.

The ActiveMQ user credentials are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file, which is located in the Sentinel server.

6 (Optional) To verify the password, see the following line in the `activemqusers.properties`

For Collector Manager:

```
collectormanager=<password>
```

In this example, `collectormanager` is the username and the corresponding value is the password.

For Correlation Engine:

```
correlationengine=<password>
```

In this example, `correlationengine` is the username and the corresponding value is the password.

7 Click **Next**.

8 Accept the certificate.

9 Click **Next** to complete the installation.

When the installation is complete, the installer displays a message indicating that this appliance is the Sentinel Collector Manager or the Sentinel Correlation Engine depending on what you chose to install, along with the IP address. It also displays the Sentinel server user interface IP address.

13.3 Post-Installation Configuration for the Appliance

After you install Sentinel, you need to perform additional configuration for the appliance to work properly.

- Section 13.3.1, “Configuring WebYaST,” on page 82
- Section 13.3.2, “Creating Partitions,” on page 82
- Section 13.3.3, “Registering for Updates,” on page 83
- Section 13.3.4, “Configuring the Appliance with SMT,” on page 83

13.3.1 Configuring WebYaST

The Sentinel appliance user interface is equipped with WebYaST, which is a Web-based remote console for controlling appliances based on SUSE Linux Enterprise. You can access, configure, and monitor the Sentinel appliances with WebYaST. The following procedure briefly describes the steps to configure WebYaST. For more information on detailed configuration, see the *WebYaST User Guide* (http://www.novell.com/documentation/webyast/).

1 Log in to the Sentinel appliance.

2 Click **Appliance**.

3 Configure the Sentinel Server to receive updates as described in Section 13.3.3, “Registering for Updates,” on page 83.

4 Click **Next** to finish the initial setup.

13.3.2 Creating Partitions

As a best practice, ensure that you create separate partitions to store Sentinel data on a different partition than the executables, configuration, and operating system files. The benefits of storing variable data separately include easier backup of sets of files, simpler recovery in case of corruption, and provides additional robustness if a disk partition fills up. For information about planning your partitions, see Section 6.6, “Planning Partitions for Data Storage,” on page 44. You can add partitions in the appliance and move a directory to the new partition by using the YaST tool.

Use the following procedure to create a new partition and move the data files from its directory to the newly created partition:

1 Log in to Sentinel as `root`.

2 Run the following command to stop the Sentinel on the appliance:

```
/etc/init.d/sentinel stop
```

3 Specify the following command to change to `novell` user:

```
su - novell
```

4 Move the contents of the directory at `/var/opt/novell/sentinel` to a temporary location.

5 Change to `root` user.

6 Enter the following command to access the YaST2 Control Center:

```
yast
```

7 Select **System > Partitioner**.

8 Read the warning and select **Yes** to add the new unused partition.

For information about creating partitions, see Using the YaST Partitioner in the *SLES 11 documentation*.

9 Mount the new partition at `/var/opt/novell/sentinel`.

10 Specify the following command to change to `novell` user:

```
su - novell
```

11 Move the contents of the data directory from the temporary location (where it was saved in Step 4) back to `/var/opt/novell/sentinel` in the new partition.

12 Run the following command to restart the Sentinel appliance:

```
/etc/init.d/sentinel start
```

13.3.3 Registering for Updates

You must register the Sentinel appliance with the appliance update channel to receive patch updates. To register the appliance, you must first obtain your appliance registration code or the appliance activation key from the NetIQ Customer Care Center.

Use the following steps to register the appliance for updates:

1 Log in to the Sentinel appliance.

2 Click **Appliance** to launch WebYaST.

3 Click **Registration**.

4 Specify the e-mail ID that you want to receive updates, then specify the system name and the appliance registration code.

5 Click **Save**.

13.3.4 Configuring the Appliance with SMT

In secured environments where the appliance must run without direct Internet access, you can configure the appliance with the Subscription Management Tool (SMT), which enables you to upgrade the appliance to the latest versions of Sentinel as they are released. SMT is a package proxy system that is integrated with NetIQ Customer Center and provides key NetIQ Customer Center capabilities.

- "Prerequisites" on page 84
- "Configuring the Appliance" on page 84
- "Upgrading the Appliance" on page 85

Prerequisites

- Get the NetIQ Customer Center credentials for Sentinel to get updates from NetIQ. For information on getting the credentials, contact NetIQ Support.
- Ensure that SLES 11 SP3 is installed with the following packages on the machine where you want to install SMT:
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - yum-metadata-parser
  - createrepo
  - perl-DBI
  - apache2-prefork
  - libapr1
  - perl-Data-ShowTable
  - perl-Net-Daemon
  - perl-Tie-IxHash
  - fltk
  - libapr-util1
  - perl-PlRPC
  - apache2-mod_perl
  - apache2-utils
  - apache2
  - perl-DBD-mysql
- Install SMT and configure the SMT server. For more information, refer to the following sections in the SMT documentation:
  - SMT Installation
  - SMT Server Configuration
  - Mirroring Installation and Update Repositories with SMT
- Install the `wget` utility on the appliance computer.

Configuring the Appliance

For information on configuring the appliance with SMT, see the Subscription Management Tool (SMT) for SUSE Linux Enterprise 11 documentation.

To enable the appliance repositories, execute the following command:

```
smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64

smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64

smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
```

Upgrading the Appliance

For information about upgrading the appliance, see Section 25.3, “Upgrading the Appliance by Using SMT,” on page 128.

13.4 Stopping and Starting the Server by Using WebYaST

You can start and stop the Sentinel server by using the Web interface as follows:

1. Log in to the Sentinel appliance.
2. Click **Appliance** to launch WebYaST.
3. Click **System Services**.
4. To stop the Sentinel server, click **stop**.
5. To start the Sentinel server, click **start**.

14 NetFlow Collector Manager Installation

You must install the NetFlow Collector Manager on a separate computer and not on the same computer where the Sentinel server, Collector Manager, or a Correlation Engine is installed.

14.1 Installation Checklist

Ensure that you have completed the following tasks before starting the installation.

- ❒ Make sure that your hardware and software meet the minimum requirements. For more information, see Chapter 5, “Meeting System Requirements,” on page 37.
- ❒ Synchronize time by using the Network Time Protocol (NTP).

14.2 Installing the NetFlow Collector Manager

You can install NetFlow Collector Managers by using one of the following methods:

- **Standard:** Uses the default values for the NetFlow configuration.
- **Custom:** Allows you to customize the port number of the Sentinel server.

NOTE

- To send network flow data to the Sentinel server, you must be an administrator, belong to the NetFlow Provider role, or have the Send NetFlow data permission.
- If you plan to install more than one NetFlow Collector Manager, you should create a new user account for each NetFlow Collector Manager to send network flow data to Sentinel. Having different user accounts for each NetFlow Collector Manager provides an additional level of control over which NetFlow Collector Managers are allowed to send data to Sentinel.

To install the NetFlow Collector Manager:

1 Launch the Sentinel Web interface by specifying the following URL in your Web interface:

```
https://<IP_Address_Sentinel_server>:8443
```

The <IP_Address_Sentinel_server> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

Log in with the user name and password specified during the installation of the Sentinel server.

2 In the toolbar, click **Downloads**.

3 Under the NetFlow Collector Manager heading, click **Download Installer**.

4 Click **Save File** to save the installer to the desired location.

5 In the command prompt, specify the following command to extract the installation file.

```
tar zxvf <install_filename>
```

Replace *<install_filename>* with the actual name of the install file.

6 Change to the directory where you extracted the installer:

```
cd <directory_name>
```

7 Specify the following command to install the NetFlow Collector Manager:

```
./install-netflow
```

8 Specify the number for the language you want to use for the installation, then press Enter.

9 Press the Spacebar to read through the license agreement.

10 Enter `yes` or `y` to accept the license and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt for the configuration type.

11 Specify whether you want to proceed with Standard or Custom installation.

12 Specify the hostname or IP address of the Sentinel server that should receive network flow data.

13 (Conditional) If you chose Custom installation, specify the port number of the Sentinel server.

The default port number is 8443.

14 Specify the user name and password to authenticate to the Sentinel server.

NOTE: Ensure that the user credentials you specify have the Send NetFlow data permission or administration privileges. Otherwise, the installation completes, but the authentication fails when the NetFlow Collector Manager sends data to the Sentinel server.

The installation completes. It might take a few minutes for the NetFlow Collector Manager to establish a connection to the Sentinel server.

15 (Optional) You can determine whether the NetFlow Collector Manager installation is successful by performing one of the following:

- Verify whether the NetFlow Collector Manager services are running:

  ```
  /etc/init.d/sentinel status
  ```

- Verify whether the NetFlow Collector Manager has established a connection with the Sentinel server:

  ```
  netstat -an |grep 'ESTABLISHED' |grep <HTTPS_port_number>
  ```

- Verify whether the NetFlow Collector Manager appears in the Sentinel Web console by clicking **Collection** > **NetFlow**.

16 Enable network flow traffic forwarding on the device from which you want to collect network flow data.

As part of enabling NetFlow on the device, you must specify the IP address of the Sentinel server and the port on which the NetFlow Collector Manager receives data from the NetFlow enabled device. The default port number is 3578. For more information, refer to the specific NetFlow enabled device documentation.

15 Installing Additional Collectors and Connectors

By default, all released Collectors and Connectors are installed when you install Sentinel. If you want to install a new Collector or Connector released after the Sentinel release, use the information in the following sections.

- Section 15.1, “Installing a Collector,” on page 89
- Section 15.2, “Installing a Connector,” on page 89

15.1 Installing a Collector

Use the following steps to install a Collector:

1. Download the desired Collector from the Sentinel Plug-ins Web site.
2. Log in to the Sentinel Web interface at https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
3. Click **applications** in the toolbar, then click **Applications**.
4. Click **Launch Control Center** to launch the Sentinel Control Center.
5. In the toolbar, click **Event Source Management** > **Live View**, then click **Tools** > **Import plugin**.
6. Browse to and select the Collector file you downloaded in Step 1, then click **Next**.
7. Follow the remaining prompts, then click **Finish**.

To configure the Collector, see the documentation for the specific Collector on the Sentinel Plug-ins Web site.

15.2 Installing a Connector

Use the following steps to install a Connector:

1. Download the desired Connector from the Sentinel Plug-ins Web site.
2. Log in to the Sentinel Web interface at https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
3. Click **application** in the toolbar, then click **Applications**.
4. Click **Launch Control Center** to launch the Sentinel Control Center.
5. In the toolbar, select **Event Source Management** > **Live View**, then click **Tools** > **Import plugin**.
6. Browse to and select the Connector file you downloaded in Step 1, then click **Next**.
7. Follow the remaining prompts, then click **Finish**.

To configure the Connector, see the documentation for the specific Connector on the Sentinel Plug-ins Web site.

16 Verifying the Installation

You can determine whether the installation is successful by performing either of the following:

- Verify the Sentinel version:

  ```
  /etc/init.d/sentinel version
  ```

- Verify whether the Sentinel services are up and running:

  ```
  /etc/init.d/sentinel status
  ```

- Verify whether the Web services are up and running:

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  The default port number is 8443.
- Access the Sentinel Web interface:
  1. Launch a supported Web browser.
  2. Specify the URL of the Sentinel Web interface:

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     IP_Address/DNS_Sentinel_server is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.
  3. Log in with the administrator name and password specified during the installation. The default username is admin.

IV Configuring Sentinel

This section provides information about configuring Sentinel and the out-of-the-box plug-ins.

17 Configuring Time

The time of an event is very critical to its processing in Sentinel. It is important for reporting and auditing purposes as well as for real-time processing. This section provides information about understanding time in Sentinel, how to configure time, and handling time zones.

17.1 Understanding Time in Sentinel

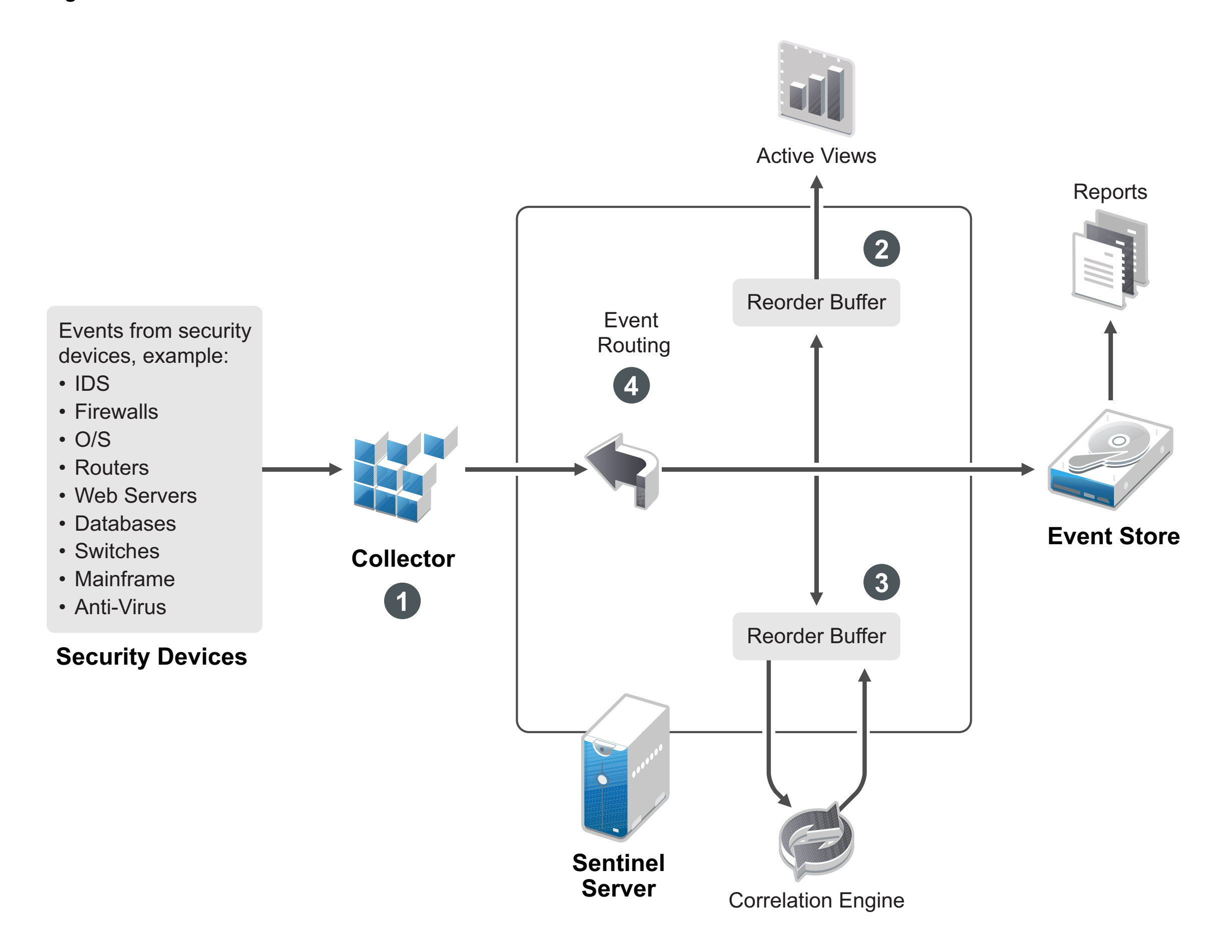
Sentinel is a distributed system that is made up of several processes distributed through out your network. In addition, there can be some delay introduced by the event source. To accommodate this, the Sentinel processes reorder events into a time-ordered stream before processing.

Every event has three time fields:

- **Event Time:** This is the event time used by all analytical engines, searches, reports, and so on.
- **Sentinel Process Time:** The time Sentinel collected the data from the device, which is taken from the Collector Manager system time.
- **Observer Event Time:** The time stamp the device put in the data. The data might not always contain a reliable time stamp and can be quite different than the Sentinel Process Time. For example, when the device delivers data in batches.

The following illustration explains how Sentinel does this:

Figure 17-1 *Sentinel Time*



1. By default, the Event Time is set to the Sentinel Process Time. The ideal, however, is for the Event Time to match the Observer Event Time, if it is available and trustworthy. It is best to configure data collection to **Trust Event Source Time** if the device time is available, accurate, and properly parsed by the Collector. The Collector sets the Event Time to match the Observer Event Time.
2. The events that have an Event Time within a 5 minute range from the server time (in the past or future) are processed normally by Active Views. Events that have an Event Time more than 5 minutes in the future do not show in the Active Views, but are inserted into the event store. Events that have an Event Time more than 5 minutes in the future and less than 24 hours in the past still are shown in the charts, but are not shown in the event data for that chart. A drill-down operation is necessary to retrieve those events from the event store.
3. Events are sorted into 30-second intervals so that the Correlation Engine can process them in chronological order. If the Event Time is more than 30 seconds older than the server time, the Correlation Engine does not process the events.
4. If the Event Time is older than 5 minutes relative to the Collector Manager system time, Sentinel directly routes events to the event store, bypassing real-time systems like Correlation, Active Views, and Security Intelligence.

17.2 Configuring Time in Sentinel

The Correlation Engine processes time-ordered streams of events and detects patterns within events as well as temporal patterns in the stream. However, sometimes the device generating the event might not include the time in its log messages. To configure time to work correctly with Sentinel, you have two options:

- Configure NTP on the Collector Manager and deselect **Trust Event Source Time** on the event source in the Event Source Manager. Sentinel uses the Collector Manager as the time source for the events.
- Select **Trust Event Source Time** on the event source in Event Source Manager. Sentinel uses the time from the log message as the correct time.

To change this setting on the event source:

1 Log in to Event Source Management.

   For more information, see "Accessing Event Source Management" in the *NetIQ Sentinel Administration Guide*.

2 Right-click the event source you want to change the time setting for, then select **Edit**.

3 Select or deselect the **Trust Event Source** option on the bottom of the **General** tab.

4 Click **OK** to save the change.

17.3 Configuring Delay Time Limit for Events

When Sentinel receives events from event sources, there may be a delay between the time the event was generated and the time Sentinel processes it. Sentinel stores the events with large delays in separate partitions. If many events are delayed over a long period of time, it may be an indicator of an incorrectly configured event source. This might also decrease the Sentinel performance as it attempts to handle the delayed events. Since the delayed events may be the result of a misconfiguration and, therefore, may not be desirable to store, Sentinel allows you to configure the acceptable delay limit for the incoming events. The event router drops the events that exceed the delay limit. Specify the delay limit in the following property in the `configuration.properties` file:

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

You can also have a listing periodically logged to the Sentinel server log file showing the event sources from which events are received that are delayed beyond a specified threshold. To log this information, specify the threshold in the following property in the `configuration.properties` file:

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

17.4 Handling Time Zones

Handling time zones can become very complex in a distributed environment. For example, you might have an event source in one time zone, the Collector Manager in another, the back-end Sentinel server in another, and the client viewing the data in yet another. When you add concerns such as daylight saving time and the many event sources that don't report what time zone they are set to

(such as all syslog sources), there are many possible problems that need to be handled. Sentinel is flexible so that you can properly represent the time when events actually occur, and compare those events to other events from other sources in the same or different time zones.

In general, there are three different scenarios for how event sources report time stamps:

- The event source reports the time in UTC. For example, all standard Windows Event Log events are always reported in UTC.
- The event source reports in local time, but always includes the time zone in the time stamp. For example, any event source that follows RFC3339 in structuring time stamps include the time zone as an offset; other sources report long time zone IDs such as Americas/New York, or short time zone IDs such as EST, which can present problems because of conflicts and inadequate resolutions.
- The event source reports local time, but does not indicate the time zone. Unfortunately, the extremely common syslog format follows this model.

For the first scenario, you can always calculate the absolute UTC time that an event occurred (assuming that a time sync protocol is in use), so you can easily compare the timing of that event to any other event source in the world. However, you cannot automatically determine what the local time was when the event occurred. For this reason, Sentinel allows customers to manually set the time zone of an event source by editing the Event Source node in the Event Source Manager and specifying the appropriate time zone. This information does not affect the calculation of DeviceEventTime or EventTime, but is placed into the ObserverTZ field, and is used to calculate the various ObserverTZ fields, such as ObserverTZHour. These fields are always expressed in local time.

In the second scenario, if the long-form time zone IDs or offsets are used, you can convert to UTC to get the absolute canonical UTC time (stored in DeviceEventTime), but you can also calculate the local time ObserverTZ fields. If a short-form time zone ID is used, there is some potential for conflicts.

The third scenario requires the administrator to manually set the event source time zone for all affected sources so that Sentinel can properly calculate the UTC time. If the time zone is not properly specified by editing the Event Source node in the Event Source Manager, then the DeviceEventTime (and probably the EventTime) can be incorrect; also, the ObserverTZ and associated fields might be incorrect.

In general, the Collector for a given type of event source (such as Microsoft Windows) knows how an event source presents time stamps, and adjusts accordingly. It is always good policy to manually set the time zone for all Event Source nodes in the Event Source Manager, unless you know that the event source reports in local time and always includes the time zone in the time stamp

Processing the event source presentation of the time stamp happens in the Collector and on the Collector Manager. The DeviceEventTime and the EventTime are stored as UTC, and the ObserverTZ fields are stored as strings set to local time for the event source. This information is sent from the Collector Manager to the Sentinel server and stored in the event store. The time zone that the Collector Manager and the Sentinel server are in should not affect this process or the stored data. However, when a client views the event in a Web browser, the UTC EventTime is converted to the local time according to the Web browser, so all events are presented to clients in the local time zone. If the users want to see the local time of the source, they can examine the ObserverTZ fields for details.

18 Modifying the Configuration after Installation

After installing Sentinel, if you want to enter the valid license key, change the password, or modify any of the assigned ports, you can run the `configure.sh` script to modify them. The script is available in the `/opt/novell/sentinel/setup` folder.

1 Shut down Sentinel using the following command:

```
rcsentinel stop
```

2 Specify the following command at the command line to run the `configure.sh` script:

```
./configure.sh
```

3 Specify `1` to perform a standard configuration or specify `2` to perform a custom configuration of Sentinel.

4 Press the Spacebar to read through the license agreement.

5 Enter `yes` or `y` to accept the license agreement and continue with the installation.

   The installation might take a few seconds to load the installation packages.

6 Enter `1` to use the default evaluation license key

   or

   Enter `2` to enter a purchased license key for Sentinel.

7 Decide whether you want to keep the existing password for the `admin` administrator user.

   - If you want to keep the existing password, enter `1`, then continue with Step 8.
   - If you want to change the existing password, enter `2`, specify the new password, confirm the password, then continue with Step 8.

     The `admin` user is the identity used to perform administration tasks through the Sentinel web console, including the creation of other user accounts.

8 Decide whether you want to keep the existing password for the `dbauser` database user.

   - If you want to keep the existing password, enter `1`, then continue with Step 9.
   - If you want to change the existing password, enter `2`, specify the new password, confirm the password, then continue with Step 9.

   The `dbauser` account is the identity that Sentinel uses to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.

9 Decide whether you want to keep the existing password for the `appuser` application user.

   - If you want to keep the existing password, enter `1`, then continue with Step 10.
   - If you want to change the existing password, enter `2`, specify the new password, confirm the password, then continue with Step 10.

     The `appuser` account is an internal identity, which Sentinel java process uses to establish connection and interact with the database. The password you enter here is used to perform database tasks.

10 Change the port assignments for the Sentinel services by entering the desired number, then specifying the new port number.

11 After you have changed the ports, specify `7` for done.

12 Enter `1` to authenticate users using only the internal database.

or

If you have configured an LDAP directory in your domain, enter `2` to authenticate users by using LDAP directory authentication.

The default value is `1`.

19 Configuring Out-of-the-Box Plug-Ins

Sentinel is preinstalled with the default Sentinel plug-ins available at the time of the Sentinel release.

This chapter provides information about how to configure the out-of-the-box plug-ins.

19.1 Viewing the Preinstalled Plug-Ins

You can see the list of plug-ins preinstalled in Sentinel. You can also see the plug-ins versions and other metadata, which helps you determine whether you have the latest version of a plug-in.

To view the plug-ins installed in your Sentinel server:

1. Log in as an administrator to the Sentinel Web interface at `https://<IP address>:8443`, where 8443 is the default port for the Sentinel server.
2. Click **Plug-ins** > **Catalog**.

19.2 Configuring Data Collection

For information about configuring Sentinel for data collection, see "Collecting and Routing Event Data" in the *NetIQ Sentinel Administration Guide*.

19.3 Configuring Solution Packs

Sentinel ships with a wide variety of useful out-of-the-box content that you can use immediately to meet many of your analysis needs. Much of this content comes from the pre-installed Sentinel Core Solution Pack and Solution Pack for ISO 27000 Series. For more information, see "Using Solution Packs" in the *NetIQ Sentinel Administration Guide*.

Solution Packs allow categorization and grouping of content into controls or policy sets that are treated as a unit. The controls in the Solution Packs are pre-installed to provide you with this out-of-the-box content, but you have to formally implement or test those controls by using the Sentinel Web console.

If a certain amount of rigor is desired to help show that your Sentinel implementation is working as designed, you may use the formal attestation process built into the Solution Packs. This attestation process implements and tests the Solution Pack controls just as you would implement and test controls from any other Solution Pack. As part of this process, the implementer and tester will attest that they have completed their work; these attestations will then become part of an audit trail that can be examined to demonstrate that any particular control was properly deployed.

You can do the attestation process by using the Solution Manager. For more information on implementing and testing the controls, see “Installing and Managing Solution Packs” in the *NetIQ Sentinel Administration Guide*.

19.4 Configuring Actions and Integrators

For information about configuring the out-of-the-box plug-ins, see the specific plug-in documentation available on the Sentinel Plug-ins Web site.

20 Enabling FIPS 140-2 Mode in an Existing Sentinel Installation

This chapter provides information about enabling FIPS 140-2 mode in an existing installation of Sentinel.

NOTE: These instructions assume that Sentinel is installed at the `/opt/novell/sentinel` directory. The commands must be executed as the `novell` user.

20.1 Enabling Sentinel Server to Run in FIPS 140-2 Mode

To enable the Sentinel Server to run in FIPS 140-2 mode:

1. Log in to the Sentinel server.
2. Switch to `novell` user (`su novell`).
3. Browse to the Sentinel bin directory.
4. Run the `convert_to_fips.sh` script and follow the on-screen instructions.
5. Complete the FIPS 140-2 mode configuration by following the tasks mentioned in Chapter 21, "Operating Sentinel in FIPS 140-2 Mode," on page 105.

20.2 Enabling FIPS 140-2 Mode on Remote Collector Managers and Correlation Engines

You must enable FIPS 140-2 mode on the remote Collector Manager and Correlation Engine if you want to use FIPS-approved communications with the Sentinel server running in FIPS 140-2 mode.

To enable a remote Collector Manager or Correlation Engine to run in FIPS 140-2 mode:

1. Login to the remote Collector Manager or Correlation Engine system.
2. Switch to `novell` user (`su novell`).
3. Browse to the bin directory. The default location is `/opt/novell/sentinel/bin`.
4. Run the `convert_to_fips.sh` script and follow the on-screen instructions.
5. Complete the FIPS 140-2 mode configuration by following the tasks mentioned in Chapter 21, "Operating Sentinel in FIPS 140-2 Mode," on page 105.

21 Operating Sentinel in FIPS 140-2 Mode

This chapter provides information about configuring and operating Sentinel in FIPS 140-2 mode.

21.1 Configuring the Advisor Service in FIPS 140-2 Mode

The Advisor service uses a secure HTTPS connection to download its feed from the Advisor server. The certificate used by the server for secure communication needs to be added to the Sentinel FIPS keystore database.

To verify successful registration with the Resource Management database:

1. Download the certificate from the Advisor server and save the file as `advisor.cer`.
2. Import the Advisor server certificate into the Sentinel FIPS keystore.

   For more information about importing the certificate, see “Importing Certificates into FIPS Keystore Database” on page 113.

21.2 Configuring Distributed Search in FIPS 140-2 Mode

This section provides information about configuring distributed search in FIPS 140-2 mode.

Scenario 1: Both the source and the target Sentinel servers are in FIPS 140-2 mode

To allow distributed searches across multiple Sentinel servers running in FIPS 140-2 mode, you need to add the certificates used for secure communication to the FIPS keystore.

1. Log in to the distributed search source computer.
2. Browse to the certificate directory:

   ```
   cd <sentinel_install_directory>/config
   ```

3. Copy the source certificate (`sentinel.cer`) to a temporary location on the target computer.
4. Import the source certificate into the target Sentinel FIPS keystore.

   For more information about importing the certificate, see “Importing Certificates into FIPS Keystore Database” on page 113.

5 Log in to the distributed search target computer.

6 Browse to the certificate directory:

```
cd /etc/opt/novell/sentinel/config
```

7 Copy the target certificate (`sentinel.cer`) to a temporary location on the source computer.

8 Import the target system certificate into the source Sentinel FIPS keystore.

9 Restart the Sentinel services on both the source and target computer.

Scenario 2: The source Sentinel server is in non-FIPS mode and the target Sentinel server is in FIPS 140-2 mode

You must convert the Web server keystore on the source computer to the certificate format and then export the certificate to the target computer.

1 Log in to the distributed search source computer.

2 Create the Web server keystore in certificate (`.cer)` format:

```
<sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 Copy the distributed search source certificate (`Sentinel.cer`) to a temporary location on the distributed search target computer.

4 Log in to the distributed search target computer.

5 Import the source certificate into the target Sentinel FIPS keystore.

For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

6 Restart Sentinel services on the target computer.

Scenario 3: The source Sentinel server is in FIPS mode and the target Sentinel server is in non-FIPS mode

1 Log in to the distributed search target computer.

2 Create the Web server keystore in certificate (.cer) format:

```
<sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
password -file <certificate_name.cer>
```

3 Copy the certificate to a temporary location on the distributed search source computer.

4 Import the target certificate into the source Sentinel FIPS keystore.

For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

5 Restart the Sentinel services on the source computer.

21.3 Configuring LDAP Authentication in FIPS 140-2 Mode

To configure LDAP authentication for Sentinel servers running in FIPS 140-2 mode:

1 Get the LDAP server certificate from the LDAP administrator, or you can use a command. For example,

```
openssl s_client -connect <LDAP server IP>:636
```

and then copy the text returned (between but not including the BEGIN and END lines) into a file.

2. Import the LDAP server certificate into the Sentinel FIPS keystore.

   For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

3. Log in to Sentinel Web console as a user in the administrator role and proceed with configuring LDAP authentication.

   For more information, see "Configuring LDAP Authentication"in the *NetIQ Sentinel Administration Guide*.

NOTE: You can also configure LDAP authentication for a Sentinel server running in FIPS 140-2 mode by running the `ldap_auth_config.sh` script in the `/opt/novell/sentinel/setup` directory.

21.4 Updating Server Certificates in Remote Collector Managers and Correlation Engines

To configure existing remote Collector Managers and Correlation Engines to communicate with a Sentinel server running in FIPS 140-2 Mode, you can either convert the remote system in FIPS 140-2 mode or you can update the Sentinel server certificate to the remote system and leave the Collector Manager or Correlation Engine in non-FIPS mode. Remote Collector Managers in FIPS mode may not work with event sources that do not support FIPS or that require one of the Sentinel Connectors that are not yet FIPS-enabled.

If you do not plan to enable FIPS 140-2 mode on the remote Collector Manager or Correlation Engine, you must copy the latest Sentinel server certificate to the remote system, so that the Collector Manager or Correlation Engine, can communicate with the Sentinel server.

To update the Sentinel server certificate in the remote Collector Manager or Correlation Engine:

1. Log in to the remote Collector Manager or Correlation Engine computer.
2. Switch to `novell` user (`su novell`).
3. Browse to the bin directory. The default location is `/opt/novell/sentinel/bin`.
4. Run the `updateServerCert.sh` script and follow the on-screen instructions.

21.5 Configuring Sentinel Plug-Ins to Run in FIPS 140-2 Mode

This section provides information about configuring various Sentinel plug-ins to run in FIPS 140-2 mode.

NOTE: These instructions assume that Sentinel is installed at the `/opt/novell/sentinel` directory. The commands must be executed as `novell` user.

21.5.1 Agent Manager Connector

Follow the below procedure only if you have selected the **Encrypted (HTTPS)** option when configuring the networking settings of the Agent Manager Event Source Server.

To configure the Agent Manager Connector to run in FIPS 140-2 mode:

1. Add or edit the Agent Manager Event Source Server. Proceed through the configuration screens until the Security window is displayed. For more information, see the *Agent Manager Connector Guide*.
2. Select one of the options from the *Client Authentication Type* field. The client authentication type determines how strictly the SSL Agent Manager Event Source Server verifies the identity of Agent Manager Event Sources that are attempting to send data.
   * **Open:** Allows all the SSL connections coming from the Agent Manager agents. Does not perform any client certificate validation or authentication.
   * **Strict:** Validates the certificate to be a valid X.509 certificate and also checks that the client certificate is trusted by the Event Source Server. New sources will need to be explicitly added to Sentinel (this prevents rogue sources from sending unauthorized data).

     For the **Strict** option, you must import the certificate of each new Agent Manager client into the Sentinel FIPS keystore. When Sentinel is running in FIPS 140-2 mode, you cannot import the client certificate using the Event Source Management (ESM) interface.

     For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

   NOTE: In FIPS 140-2 mode, the Agent Manager Event Source Server uses the Sentinel server key pair; importing the server key pair is not required.

   ---
3. If server authentication is enabled in the agents, the agents must additionally be configured to trust the Sentinel server or the remote Collector Manager certificate depending on where the Connector is deployed.

   Sentinel server certificate location: `/etc/opt/novell/sentinel/config/sentinel.cer`

   Remote Collector Manager certificate location: `/etc/opt/novell/sentinel/config/rcm.cer`

   NOTE: When using custom certificates that are digitally signed by a certificate authority (CA), the Agent Manager agent must trust the appropriate certificate file.

21.5.2 Database (JDBC) Connector

Follow the below procedure only if you have selected the *SSL* option when configuring the database connection.

To configure the Database Connector to run in FIPS 140-2 mode:

1. Before configuring the Connector, download the certificate from the Database server and save it as `database.cert` file into the `/etc/opt/novell/sentinel/config` directory of the Sentinel server.

   For more information, refer to the respective database documentation.

2. Import the certificate into the Sentinel FIPS keystore.

   For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

3. Proceed with configuring the Connector.

21.5.3 Sentinel Link Connector

Follow the below procedure only if you have selected **Encrypted (HTTPS)** option when configuring the networking settings of the Sentinel Link Event Source Server.

To configure the Sentinel Link Connector to run in FIPS 140-2 mode:

1. Add or edit the Sentinel Link Event Source Server. Proceed through the configuration screens until the Security window is displayed. For more information, see the *Sentinel Link Connector Guide*.

2. Select one of the options from the *Client Authentication Type* field. The client authentication type determines how strictly the SSL Sentinel Link Event Source Server verifies the identity of Sentinel Link Event Sources (Sentinel Link Integrators) that are attempting to send data.

   - **Open:** Allows all the SSL connections coming from the clients (Sentinel Link Integrators). Does not perform any Integrator certificate validation or authentication.
   - **Strict:** Validates the Integrator certificate to be a valid X.509 certificate and also checks that the Integrator certificate is trusted by the Event Source Server. For more information, refer to the respective database documentation.

     For the **Strict** option:

     - If the Sentinel Link Integrator is in FIPS 140-2 mode, you must copy the `/etc/opt/novell/sentinel/config/sentinel.cer` file from the sender Sentinel machine to the receiver Sentinel machine. Import this certificate into the receiver Sentinel FIPS keystore.

       NOTE: When using custom certificates that are digitally signed by a certificate authority (CA), you must import the appropriate custom certificate file.

     - If Sentinel Link Integrator is in non-FIPS mode, you must import the custom Integrator certificate into the receiver Sentinel FIPS keystore.

NOTE: If the sender is Sentinel Log Manager (in non-FIPS mode) and the receiver is Sentinel in FIPS 140-2 mode, the server certificate to be imported on the sender is the `/etc/opt/novell/sentinel/config/sentinel.cer` file from the receiver Sentinel machine.

When Sentinel is running in FIPS 140-2 mode, you cannot import the client certificate using the Event Source Management (ESM) interface. For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

NOTE: In FIPS 140-2 mode, the Sentinel Link Event Source server uses the Sentinel server key pair. Importing the server key pair is not required.

21.5.4 Syslog Connector

Follow the below procedure only if you have selected the **SSL** protocol when configuring the network settings of the Syslog Event Source Server.

To configure the Syslog Connector to run in FIPS 140-2 mode:

1 Add or edit the Syslog Event Source Server. Proceed through the configuration screens until the Networking window is displayed. For more information, see the *Syslog Connector Guide*.

2 Click **Settings**.

3 Select one of the options from the *Client Authentication Type* field. The client authentication type determines how strictly the SSL Syslog Event Source Server verifies the identity of Syslog Event Sources that are attempting to send data.

- **Open:** Allows all the SSL connections coming from the clients (event sources). Does not perform any client certificate validation or authentication.
- **Strict:** Validates the certificate to be a valid X.509 certificate and also checks that the client certificate is trusted by the Event Source Server. New sources will have to be explicitly added to Sentinel (this prevents rogue sources from sending data to Sentinel).

  For the **Strict** option, you must import the certificate of the syslog client into the Sentinel FIPS keystore.

  When Sentinel is running in FIPS 140-2 mode, you cannot import the client certificate using the Event Source Management (ESM) interface.

  For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

NOTE: In FIPS 140-2 mode, the Syslog Event Source Server uses the Sentinel server key pair. Importing the server key pair is not required.

4 If server authentication is enabled in the syslog client, the client must trust the Sentinel server certificate or the remote Collector Manager certificate depending on where the Connector is deployed.

The Sentinel server certificate file is in the `/etc/opt/novell/sentinel/config/sentinel.cer` location.

The Remote Collector Manger certificate file is in `/etc/opt/novell/sentinel/config/rcm.cer` location.

NOTE: When using custom certificates that are digitally signed by a certificate authority (CA), the client must trust the appropriate certificate file.

21.5.5 Windows Event (WMI) Connector

To configure the Windows Event (WMI) Connector to run in FIPS 140-2 mode:

1. Add or edit the Windows Event Connector. Proceed through the configuration screens until the Security window is displayed. For more information, see the *Windows Event (WMI) Connector Guide*.
2. Click **Settings**.
3. Select one of the options from the *Client Authentication Type* field. The client authentication type determines how strictly the Windows Event Connector verifies the identity of the client Windows Event Collection Services (WECS) that are attempting to send data.
   - **Open:** Allows all the SSL connections coming from the client WECS. Does not perform any client certificate validation or authentication.
   - **Strict:** Validates the certificate to be a valid X.509 certificate and also checks that the client WECS certificate is signed by a CA. New sources will need to be explicitly added (this prevents rogue sources from sending data to Sentinel).

     For the **Strict** option, you must import the certificate of the client WECS into the Sentinel FIPS keystore. When Sentinel is running in FIPS 140-2 mode, you cannot import the client certificate using the Event Source Management (ESM) interface.

     For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

   NOTE: In FIPS 140-2 mode, the Windows Event Source Server uses the Sentinel server key pair. Importing the server key pair is not required.

   ---
4. If server authentication is enabled in the Windows client, the client must trust the Sentinel server certificate or the remote Collector Manager certificate depending on where the Connector is deployed.

   The Sentinel server certificate file is in the `/etc/opt/novell/sentinel/config/sentinel.cer` location.

   The remote Collector Manager certificate file is in the `/etc/opt/novell/sentinel/config/rcm.cer` location.

   NOTE: When using custom certificates that are digitally signed by a certificate authority (CA), the client must trust the appropriate certificate file.

   ---
5. If you want to automatically synchronize the event sources or populate the list of event sources using an Active Directory connection, you must import the Active Directory server certificate into the Sentinel FIPS keystore.

   For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.

21.5.6 Sentinel Link Integrator

Follow the below procedure only if you have selected the **Encrypted (HTTPS)** option when configuring the network settings of the Sentinel Link Integrator.

To configure the Sentinel Link Integrator to run in FIPS 140-2 mode:

1. When Sentinel Link Integrator is in FIPS 140-2 mode, server authentication is mandatory. Before configuring the Integrator instance, import the Sentinel Link Server certificate into the Sentinel FIPS keystore:
   - **If Sentinel Link Connector is in FIPS 140-2 mode**:

     If the Connector is deployed in the Sentinel server, you must copy the `/etc/opt/novell/sentinel/config/sentinel.cer` file from the receiver Sentinel machine to the sender Sentinel machine.

     If the Connector is deployed in a remote Collector Manager, you must copy the `/etc/opt/novell/sentinel/config/rcm.cer file` from the receiver remote Collector Manager machine to the receiver Sentinel machine.

     Import this certificate into the sender Sentinel FIPS keystore.

     NOTE: When using custom certificates that are digitally signed by a certificate authority (CA), you must import the appropriate custom certificate file.
   - If Sentinel Link Connector is in non-FIPS mode:

     Import the custom Sentinel Link Server certificate into the sender Sentinel FIPS keystore.

     NOTE: When the Sentinel Link integrator is in FIPS 140-2 mode and the Sentinel Link Connector is in non-FIPS mode, use the custom server key pair on the connector. Do not use the internal server key pair.

   For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.
2. Proceed with configuring the Integrator instance.

   NOTE: In FIPS 140-2 mode, the Sentinel Link Integrator uses the Sentinel server key pair. Importing the Integrator key pair is not required.

21.5.7 LDAP Integrator

To configure the LDAP Integrator to run in FIPS 140-2 mode:

1. Before configuring the Integrator instance, download the certificate from the LDAP server and save it as `ldap.cert` file into the `/etc/opt/novell/sentinel/config` directory of the Sentinel server.

   For example, use

   ```
   openssl s_client -connect <LDAP server IP>:636
   ```

   and then copy the text returned (between but not including the BEGIN and END lines) into a file.
2. Import the certificate into the Sentinel FIPS keystore.

   For more information about importing the certificate, see "Importing Certificates into FIPS Keystore Database" on page 113.
3. Proceed with configuring the Integrator instance.

21.5.8 SMTP Integrator

The SMTP Integrator supports FIPS 140-2 from version 2011.1r2 and later. No configuration changes are required.

21.5.9 Using Non-FIPS Enabled Connectors with Sentinel in FIPS 140-2 Mode

This section provides information about how to use non-FIPS enabled Connectors with a Sentinel server in FIPS 140-2 mode. We recommend this approach if you have sources that do not support FIPS or if you want to collect events from the non-FIPS Connectors in your environment.

To use non-FIPS connectors with Sentinel in FIPS 140-2 mode:

1 Install a remote Collector Manager in non-FIPS mode to connect to the Sentinel server in FIPS 140-2 mode.

For more information, see Section 12.4, “Installing Collector Managers and Correlation Engines,” on page 71.

2 Deploy the non-FIPS Connectors specifically to the non-FIPS remote Collector Manager.

NOTE: There are some known issues when non-FIPS Connectors such as Audit Connector and File Connector are deployed on a non-FIPS remote Collector Manager connected to a Sentinel server in FIPS 140-2 mode. For more information about these known issues, see the Sentinel 7.1 Release Notes.

21.6 Importing Certificates into FIPS Keystore Database

You must insert certificates into the Sentinel FIPS keystore database to establish secure (SSL) communications from the components that own those certificates to Sentinel. You cannot upload certificates by using the Sentinel user interface as normal when FIPS 140-2 mode is enabled in Sentinel. You must manually import the certificates into the FIPS keystore database.

For event sources that are using Connectors deployed to a remote Collector Manager, you must import the certificates to the FIPS keystore database of the remote Collector Manager rather than the central Sentinel server.

To import certificates to the FIPS Keystore Database:

1 Copy the certificate file to any temporary location on the Sentinel server or remote Collector Manager.

2 Browse to the Sentinel bin directory. The default location is `/opt/novell/sentinel/bin`.

3 Run the following command to import the certificate into the FIPS keystore database, and then follow the on-screen instructions:.

```
./convert_to_fips.sh -i <certificate file path>
```

4 Enter `yes` or `y` when prompted to restart the Sentinel server or remote Collector Manager.

21.7 Reverting Sentinel to Non-FIPS Mode

This section provides information about how to revert Sentinel and its components to non-FIPS mode.

- Section 21.7.1, "Reverting Sentinel Server to Non-FIPS mode," on page 114
- Section 21.7.2, "Reverting Remote Collector Managers or Remote Correlation Engines to Non-FIPS mode," on page 114

21.7.1 Reverting Sentinel Server to Non-FIPS mode

You can revert a Sentinel server running in FIPS 140-2 mode to non-FIPS mode only if you have taken a backup of your Sentinel server before converting it to run in FIPS 140-2 mode.

NOTE: When you revert a Sentinel server to non-FIPS mode, you will lose the events, incident data, and configuration changes made to your Sentinel server after converting to run FIPS 140-2 mode. The sentinel system will be restored back to the last restoration point of non-FIPS mode. You should take a backup of the current system before reverting to non-FIPS mode for future use.

To revert your Sentinel server to non-FIPS mode:

1 Log in to the Sentinel server as the `root` user.

2 Switch to the `novell` user.

3 Browse to the Sentinel bin directory. The default location is `/opt/novell/sentinel/bin`.

4 Run the following command to revert your Sentinel server to non-FIPS mode, and follow the on-screen instructions:

```
./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
```

For example, if `non-fips2013012419111359034887.tar.gz` is the backup file, run the following command:

```
./backup_util.sh -f non-fips2013012419111359034887.tar.gz -m 'restore'
```

5 Restart the Sentinel server.

21.7.2 Reverting Remote Collector Managers or Remote Correlation Engines to Non-FIPS mode

You can revert remote Collector Managers or remote Correlation Engines to non-FIPS mode.

To revert a remote Collector Managers or a remote Correlation Engine to non-FIPS mode:

1 Login to the remote Collector Manager or remote Correlation Engine system.

2 Switch to `novell` user (`su novell`).

3 Browse to the bin directory. The default location is `/opt/novell/sentinel/bin`.

4 Run the `revert_to_nonfips.sh` script and follow the on-screen instructions.

5 Restart the remote Collector Manager or remote Correlation Engine.

V Upgrading Sentinel

This section provides information about upgrading Sentinel and other components.

22 Implementation Checklist

Before you upgrade Sentinel, review the following checklist to ensure a successful upgrade:

***Table 22-1** Implementation Checklist*

❐	Tasks	See
❐	Ensure that the computers on which you install Sentinel and its components meet the specified requirements.	NetIQ Sentinel Technical Information Website
❐	Review the supported operating system release notes to understand the known issues.	SUSE Release Notes
❐	Review the Sentinel release notes to see new functionality and understand the known issues.	Sentinel Release Notes

23 Prerequisites

23.1 Prerequisite for Sentinel in FIPS Mode

The following prerequisite is applicable if you have downgraded the Java version by using JRE 7 update 45 to resolve connection problems between clients and Sentinel running in FIPS mode as mentioned in Sentinel 7.2.2 Known Issues.

If there are symbolic links in any of the Sentinel installation directories, the Sentinel installer does not continue with the upgrade. When you download and install JRE 7 update 45 to downgrade the Java version, the JRE folder contains a subfolder named `man`, which has symbolic links. Therefore, you should delete the `man` folder to upgrade successfully to Sentinel 7.3 and later. However, if you have downloaded and installed JDK 7 update 45 instead of JRE 7 update 45, the `man` folder will not contain symbolic links and the man folder need not be deleted.

To delete the man folder:

1. Log in to the Sentinel server as novell user.
2. Specify the following command to change the directory:
   ```
   cd /opt/novell/sentinel/jre/
   ```
3. Delete the `man` folder:
   ```
   rm -rf man
   ```

23.2 Prerequisite for Versions Prior to Sentinel 7.1.1

Sentinel 7.1.1 and later includes MongoDB version 2.4.1. MongoDB 2.4 requires removal of duplicate user names in the database. If you are upgrading Sentinel versions prior to 7.1.1, verify whether there are any duplicate users and then remove the duplicate users.

Perform the following steps to identify duplicate users:

1. Log in to the Sentinel 7.1 or earlier server as the novell user.
2. Change to the following directory:
   ```
   cd opt/novell/sentinel/3rdparty/mongodb/bin
   ```
3. Run the following commands to verify duplicate users:
   ```
   ./mongo --port 27017 --host "localhost"
   use analytics
   db.system.users.find().count()
   ```
   If the `count` is more than 1, it indicates there are duplicate users.

Perform the following steps to remove duplicate users:

1. Run the following command to list the users:

   ```
   db.system.users.find().pretty()
   ```

   The command lists users along with duplicate entries. The first user in the list is the original user. You should keep the first user and delete the others in the list.

2. Run the following command to remove duplicate users:

   ```
   db.system.users.remove({ _id : ObjectId("object_ID") })
   ```

3. Run the following command to verify whether the duplicate users have been removed:

   ```
   db.system.users.find().pretty()
   ```

4. Switch to database admin user:

   ```
   use admin
   ```

5. Repeat Step 1 through Step 3 to verify and remove duplicate `dbausers` in the admin database.

24 Upgrading Sentinel Traditional Installation

24.1 Upgrading Sentinel

Use the following steps to upgrade the Sentinel server:

1 Back up your configuration, then create an ESM export.

For more information on backing up data, see "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide*.

2 (Conditional) If you have customized the configuration settings in the `server.xml`, `collector_mgr.xml`, or `correlation_engine.xml` files, ensure that you have created appropriate properties files named with the obj-component id to ensure that the customizations are retained after the upgrade. For more information, see "Maintaining Custom Settings in XML Files" in the *NetIQ Sentinel Administration Guide*.

3 Download the latest installer from the NetIQ download Website.

4 Log in as `root` to the server where you want to upgrade Sentinel.

5 Specify the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

Replace *<install_filename>* with the actual name of the install file.

6 Change to the directory where the install file was extracted.

7 Specify the following command to upgrade Sentinel:

```
./install-sentinel
```

8 To proceed with a language of your choice, select the number next to the language.

The end user license agreement is displayed in the selected language.

9 Read the end user license, enter `yes` or `y` to accept the license, then continue with the installation.

10 The installation script detects that an older version of the product already exists and prompts you to specify if you want to upgrade the product. To continue with the upgrade, press y.

The installation starts installing all RPM packages. This installation might take a few seconds to complete.

11 Clear your Web browser cache to view the latest Sentinel version.

12 Clear the Java Web Start cache on the client computers to use the latest version of Sentinel applications.

You can clear the Java Web Start cache by either using the `javaws -clearcache` command or by using Java Control Center. For more information, see http://www.java.com/en/download/help/plugin_cache.xml.

13 (Conditional) If the PostgreSQL database has been upgraded to a major version (for example, 8.0 to 9.0 or 9.0 to 9.1), clear the old PostgreSQL files from the PostgreSQL database. For information about whether the PostgreSQL database was upgraded, see the Sentinel Release Notes.

   13a Switch to the novell user.

   ```
   su novell
   ```

   13b Browse to the `bin` folder:

   ```
   cd /opt/novell/sentinel/3rdparty/postgresql/bin
   ```

   13c Delete all the old postgreSQL files by using the following command:

   ```
   ./delete_old_cluster.sh
   ```

14 (Conditional) If you are upgrading from Sentinel 7.1.1 or earlier, the installer does not migrate the security intelligence (SI) data by default. To migrate SI data from Sentinel 7.1.1 or earlier, manually enable SI data migration as follows:

   14a Switch to novell user.

   ```
   su novell
   ```

   14b Open the `/etc/opt/novell/sentinel/config/server.xml` file.

   14c Add the following property in the `BaseliningRuntime` component section:

   ```
   <property name="baselining.migration.check">true</property>
   ```

   14d Restart the Sentinel server.

15 To upgrade Collector Manager systems and Correlation Engine systems, see Section 24.3, "Upgrading the Collector Manager or the Correlation Engine," on page 124.

24.2 Upgrading Sentinel as a Non-root User

If your organizational policy does not allow you to run the full upgrade of Sentinel as `root`, you can upgrade Sentinel as another user. In this upgrade, a few steps are performed as a `root` user, then you proceed to upgrade Sentinel as another user created by the `root` user.

1 Back up your configuration, then create an ESM export.

   For more information on backing up data, see "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide*.

2 (Conditional) If you have customized the configuration settings in the `server.xml`, `collector_mgr.xml`, or `correlation_engine.xml` files, ensure that you have created appropriate properties files named with the obj-component id to ensure that the customizations are retained after the upgrade. For more information, see "Maintaining Custom Settings in XML Files" in the *NetIQ Sentinel Administration Guide*.

3 Download the installation files from the NetIQ Downloads Website.

4 Specify the following command at the command line to extract the install files from the tar file:

   ```
   tar -zxvf <install_filename>
   ```

   Replace *<install_filename>* with the actual name of the install file.

5 Log in as `root` to the server where you want to upgrade Sentinel.

6 Extract the `squashfs` RPM from the Sentinel install files.

7 Install the `squashfs` on the Sentinel server.

```
rpm -Uvh <install_filename>
```

8 Specify the following command to change to the newly created non-root `novell` user: `novell`:

```
su novell
```

9 (Conditional) To do an interactive upgrade:

9a Specify the following command:

```
./install-sentinel
```

To upgrade Sentinel in a non-default location, specify the --location option along with the command. For example:.

```
./install-sentinel --location=/foo
```

9b Continue with Step 11.

10 (Conditional) To do a silent upgrade, specify the following command:

```
./install-sentinel -u <response_file>
```

The installation proceeds with the values stored in the response file. The Sentinel upgrade is complete.

11 Specify the number for the language you want to use for the upgrade.

The end user license agreement is displayed in the selected language.

12 Read the end user license and enter `yes` or `y` to accept the license and continue with the upgrade.

The upgrade starts installing all RPM packages. This installation might take a few seconds to complete.

13 Clear your Web browser cache to view the latest Sentinel version.

14 Clear the Java Web Start cache on the client computers to use the latest version of Sentinel applications.

You can clear the Java Web Start cache by either using the `javaws -clearcache` command or by using Java Control Center. For more information, see http://www.java.com/en/download/help/plugin_cache.xml.

15 (Conditional) If the PostgreSQL database has been upgraded to a major version (for example, 8.0 to 9.0 or 9.0 to 9.1), clear the old PostgreSQL files from the PostgreSQL database. For information about whether the PostgreSQL database was upgraded, see the Sentinel Release Notes.

15a Switch to novell user.

```
su novell
```

15b Browse to the `bin` folder:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c Delete all the old postgreSQL files by using the following command:

```
./delete_old_cluster.sh
```

16 (Conditional) If you are upgrading from Sentinel 7.1.1 or earlier, the installer does not migrate the security intelligence (SI) data by default. To migrate SI data from Sentinel 7.1.1 or earlier, manually enable SI data migration as follows:

16a Switch to novell user.

```
su novell
```

16b Open the `/etc/opt/novell/sentinel/config/server.xml` file.

16c Add the following property in the `BaseliningRuntime` component section:

```
<property name="baselining.migration.check">true</property>
```

16d Restart the Sentinel server.

24.3 Upgrading the Collector Manager or the Correlation Engine

Use the following steps to upgrade the Collector Manager or the Correlation Engine:

1 Back up Chapter 24, "Upgrading Sentinel Traditional Installation," on page 121your configuration and create an ESM export.

For more information, see "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide*.

2 Log in to the Sentinel Web interface as a user in the administrator role.

3 Select **Downloads**.

4 Click **Download Installer** in the Collector Manager Installer section.

A window is displayed with options to either open or to save the installer file on the local machine.

5 Save the file.

6 Copy the file to a temporary location.

7 Extract the contents of the file.

8 Run the following script:

For Collector Manager:

```
./install-cm
```

For Correlation Engine:

```
./install-ce
```

9 Follow the on-screen instructions to complete the installation.

25 Upgrading the Sentinel Appliance

The procedures in this chapter guide you through upgrading the Sentinel appliance as well as Collector Manager and Correlation Engine appliances.

25.1 Upgrading the Appliance by Using zypper

To upgrade the appliance by using the zypper patch:

1. Back up your configuration, then create an ESM export. For more information, see "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide*.
2. (Conditional) If you have customized the configuration settings in the `server.xml`, `collector_mgr.xml`, or `correlation_engine.xml` files, ensure that you have created appropriate properties files named with the obj-component id to ensure that the customizations are retained after the upgrade. For more information, see "Maintaining Custom Settings in XML Files" in the *NetIQ Sentinel Administration Guide*.
3. Log in to the appliance console as the `root` user.
4. Run the following command:

   ```
   /usr/bin/zypper patch
   ```

5. (Conditional) If you are upgrading from Sentinel 7.0.1 or earlier, enter `1` to accept the vendor change from Novell to NetIQ.
6. (Conditional) If you are upgrading from Sentinel versions prior to 7.2, the installer displays a message that indicates to resolve dependency for some appliance packages. Enter `1` for deinstallation of dependent packages.
7. Enter `Y` to proceed.
8. Enter `yes` to accept the license agreement.
9. Restart the Sentinel appliance.
10. Clear your Web browser cache to view the latest Sentinel version.
11. Clear the Java Web Start cache on the client computers to use the latest version of Sentinel applications.

    You can clear the Java Web Start cache by either using the `javaws -clearcache` command or by using Java Control Center. For more information, see http://www.java.com/en/download/help/plugin_cache.xml.
12. (Conditional) If the PostgreSQL database has been upgraded to a major version (for example, 8.0 to 9.0 or 9.0 to 9.1), clear the old PostgreSQL files from the PostgreSQL database. For information about whether the PostgreSQL database was upgraded, see the Sentinel Release Notes.

    12a Switch to novell user.

    ```
    su novell
    ```

12b Browse to the `bin` folder:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

12c Delete all the old postgreSQL files by using the following command:

```
./delete_old_cluster.sh
```

13 (Conditional) If you are upgrading from Sentinel 7.1.1 or earlier, the installer does not migrate the security intelligence (SI) data by default. To migrate SI data from Sentinel 7.1.1 or earlier, manually enable SI data migration as follows:

13a Switch to novell user.

```
su novell
```

13b Open the `/etc/opt/novell/sentinel/config/server.xml` file.

13c Add the following property in the `BaseliningRuntime` component section:

```
<property name="baselining.migration.check">true</property>
```

13d Restart the Sentinel server.

NOTE: To upgrade the Collector Manager or Correlation Engine, follow Step 3 through Step 9.

25.2 Upgrading the Appliance through WebYaST

NOTE: Appliance upgrades from versions prior to Sentinel 7.2 must be done using the zypper command line utility because user interaction is required to complete the upgrade. WebYaST is not capable of facilitating the required user interaction. For information about using zypper to upgrade the appliance, see Section 25.1, “Upgrading the Appliance by Using zypper,” on page 125.

---

1. Log in to the Sentinel appliance as a user in the administrator role.
2. Back up your configuration, then create an ESM export. For more information, see “Backing Up and Restoring Data” in the *NetIQ Sentinel Administration Guide*.
3. (Conditional) If you have customized the configuration settings in the `server.xml`, `collector_mgr.xml`, or `correlation_engine.xml` files, ensure that you have created appropriate properties files named with the obj-component id to ensure that the customizations are retained after the upgrade. For more information, see “Maintaining Custom Settings in XML Files” in the *NetIQ Sentinel Administration Guide*.
4. **If you want to upgrade the Sentinel Appliance**, click **Appliance** to launch WebYaST.
5. **If you want to upgrade a Collector Manager or Correlation Engine Appliance**, specify the URL of the Collector Manager or Correlation Engine computer using port 4984 to launch WebYaST as `https://<IP_address>:4984`, where `<IP_address>` is the IP address of the Collector Manager or Correlation Engine. Complete Step 7 through Step 10.
6. Back up your configuration, then create an ESM export.

   For more information on backing up data, see “Backing Up and Restoring Data” in the *NetIQ Sentinel Administration Guide*.
7. (Conditional) If you have not already registered the appliance for automatic updates, register for updates.

   For more information, see Section 13.3.3, “Registering for Updates,” on page 83.

If the appliance is not registered, Sentinel displays a yellow warning that indicates that the appliance is not registered.

8 To check if there are any updates, click **Updates**.

The available updates are displayed.

9 Select and apply the updates.

The updates might take a few minutes to complete. After the update is successful, the WebYaST login page is displayed.

Before upgrading the appliance, WebYaST automatically stops the Sentinel service. You must manually restart this service after the upgrade is complete.

10 Restart the Sentinel service by using the Web interface.

For more information, see Section 13.4, “Stopping and Starting the Server by Using WebYaST,” on page 85.

11 Clear your Web browser cache to view the latest Sentinel version.

12 Clear the Java Web Start cache on the client computers to use the latest version of Sentinel applications.

You can clear the Java Web Start cache by either using the `javaws -clearcache` command or by using Java Control Center. For more information, see http://www.java.com/en/download/help/plugin_cache.xml.

13 (Conditional) If the PostgreSQL database has been upgraded to a major version (for example, 8.0 to 9.0 or 9.0 to 9.1), clear the old PostgreSQL files from the PostgreSQL database. For information about whether the PostgreSQL database was upgraded, see the Sentinel Release Notes.

13a Switch to novell user.

```
su novell
```

13b Browse to the `bin` folder:

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

13c Delete all the old postgreSQL files by using the following command:

```
./delete_old_cluster.sh
```

14 (Conditional) If you are upgrading from Sentinel 7.1.1 or earlier, the installer does not migrate the security intelligence (SI) data by default. To migrate SI data from Sentinel 7.1.1 or earlier, manually enable SI data migration as follows:

14a Switch to novell user:

```
su novell
```

14b Open the `/etc/opt/novell/sentinel/config/server.xml` file.

14c Add the following property in the `BaseliningRuntime` component section:

```
<property name="baselining.migration.check">true</property>
```

14d Restart the Sentinel server.

25.3 Upgrading the Appliance by Using SMT

In secured environments where the appliance must run without direct internet access, you can configure the appliance with Subscription Management Tool (SMT) that allows you upgrade the appliance to the latest available versions.

1. Ensure that the appliance is configured with SMT.

   For more information, see Section 13.3.4, “Configuring the Appliance with SMT,” on page 83.
2. Back up your configuration, then create an ESM export. For more information, see “Backing Up and Restoring Data” in the *NetIQ Sentinel Administration Guide*.
3. (Conditional) If you have customized the configuration settings in the `server.xml`, `collector_mgr.xml`, or `correlation_engine.xml` files, ensure that you have created appropriate properties files named with the obj-component id to ensure that the customizations are retained after the upgrade. For more information, see “Maintaining Custom Settings in XML Files” in the *NetIQ Sentinel Administration Guide*.
4. Log in to the appliance console as the `root` user.
5. Refresh the repository for upgrade:

   ```
   zypper ref -s
   ```
6. Check whether the appliance is enabled for upgrade:

   ```
   zypper lr
   ```
7. (Optional) Check the available updates for the appliance:

   ```
   zypper lu
   ```
8. (Optional) Check the packages that include the available updates for the appliance:

   ```
   zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
   ```
9. Update the appliance:

   ```
   zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
   ```
10. Restart the appliance.

    ```
    rcsentinel restart
    ```

26 Upgrading Sentinel Plug-Ins

The upgrade installations of Sentinel do not upgrade the plug-ins unless a particular plug-in is not compatible with the latest version of Sentinel.

New and updated Sentinel plug-ins, including Solution Packs, are frequently uploaded to the Sentinel Plug-ins Web site. To get the latest bug fixes, documentation updates, and enhancements for a plug-in, download and install the latest version of the plug-in. For information about installing a plug-in, see the specific plug-in documentation.

VI Deploying Sentinel for High Availability

You can use this appendix to install NetIQ Sentinel in an Active-Passive High Availability mode, which allows Sentinel to fail over to a redundant cluster node in case of hardware or software failure. For more information on implementing high availability and disaster recovery in your Sentinel environment, contact NetIQ Support.

NOTE: High Availability (HA) configuration is supported only on the Sentinel server. However, Collector Managers and Correlation Engines can still communicate with the Sentinel HA server.

---

27 Concepts

High availability refers to a design methodology that is intended to keep a system available for use as much as is practicable. The intent is to minimize the causes of downtime such as system failures and maintenance, and to minimize the time it will take to detect and recover from downtime events that do occur. In practice, automated means of detecting and recovering from downtime events quickly become necessary as higher levels of availability must be achieved.

27.1 External Systems

Sentinel is a complex multi-tier application that depends upon and provides a wide variety of services. Additionally, it integrates with multiple external third-party systems for data collection, data sharing, and incident remediation. Most HA solutions allow implementors to declare dependencies between the services that should be highly available, but this only applies to services running on the cluster itself. Systems external to Sentinel such as event sources must be configured separately to be as available as required by the organization, and must also be configured to properly handle situations where Sentinel is unavailable for some period of time such as a failover event. If access rights are tightly restricted, for example if authenticated sessions are used to send and/or receive data between the third-party system and Sentinel, the third-party system must be configured to accept sessions from or initiate sessions to any cluster node (Sentinel should be configured with a virtual IP for this purpose).

27.2 Shared Storage

All HA clusters require some form of shared storage so that application data can be quickly moved from one cluster node to another, in case of a failure of the originating node. The storage itself should be highly available; this is usually achieved by using Storage Area Network (SAN) technology connected to the cluster nodes using a Fibre Channel network. Other systems use Network Attached Storage (NAS), iSCSI, or other technologies that allow for remote mounting of shared storage. The fundamental requirement of the shared storage is that the cluster can cleanly move the storage from a failed cluster node to a new cluster node.

NOTE: For iSCSI, you should use the largest Message Transfer Unit (MTU) supported by your hardware. Larger MTUs benefits the storage performance. Sentinel might experience issues if latency and bandwidth to storage is slower than recommended.

There are two basic approaches that Sentinel can use for the shared storage. The first locates all components (application binaries, configuration, and event data) on the shared storage. On failover, the storage is unmounted from the primary node and moved the backup node; which loads the entire application and configuration from the shared storage. The second approach stores the event data on shared storage, but the application binaries and configuration reside on each cluster node. On failover, only the event data is moved to the backup node.

Each approach has benefits and disadvantages, but the second approach allows the Sentinel installation to use standard FHS-compliant install paths, allows for verification of the RPM packaging, and also allows for warm patching and reconfiguration to minimize downtime.

This solution will guide you through an example of the process of installing to a cluster that uses iSCSI shared storage and locates the application binaries/configuration on each cluster node.

27.3 Service Monitoring

A key component of any highly available environment is a reliable, consistent way to monitor the resource(s) that should be highly available, along with any resource(s) that they depend on. The SLE HAE uses a component called a Resource Agent to perform this monitoring - the Resource Agent's job is to provide the status for each resource, plus (when asked) to start or stop that resource.

Resource Agents must provide a reliable status for monitored resources in order to prevent unnecessary downtime. False positives (when a resource is deemed to have failed, but would in fact recover on its own) can cause service migration (and related downtime) when it is not actually necessary, and false negatives (when the Resource Agent reports that a resource is functioning when in fact it is not operating properly) can prevent proper use of the service. On the other hand, external monitoring of a service can be quite difficult - a web service port might respond to a simple ping, for example, but may not provide correct data when a real query is issued. In many cases, self-test functionality must be built into the service itself to provide a truly accurate measurement.

This solution provides a basic OCF Resource Agent for Sentinel that can monitor for major hardware, operating system, or Sentinel system failure. At this time the external monitoring capabilities for Sentinel are based on IP port probes, and there is some potential for false positive and false negative readings. We plan to improve both Sentinel and the Resource Agent over time to improve the accuracy of this component.

27.4 Fencing

Within an HA cluster, critical services are constantly monitored and restarted automatically on other nodes in the case of failure. This automation can introduce problems, however, if some communications problem occurs with the primary node; although the service running on that node appears to be down, it in fact continues to run and write data to the shared storage. In this case, starting a new set of services on a backup node could easily cause data corruption.

Clusters use a variety of techniques collectively called fencing to prevent this from happening, including Split Brain Detection (SBD) and Shoot The Other Node In The Head (STONITH). The primary goal is to prevent data corruption on the shared storage.

28 System Requirements

When allocating cluster resources to support a high availability (HA) installation, consider the following requirements:

- ❒ **(Conditional) For HA appliance installations**, ensure that the Sentinel HA appliance with a valid license is available. The Sentinel HA appliance is an ISO appliance that includes the following packages:
  - SUSE Linux Enterprise Server (SLES) 11 SP3 operating system
  - SUSE Linux Enterprise Server High Availability Extension (SLES HAE) package
  - Sentinel software (including HA rpm)
- ❒ **(Conditional) For traditional HA installations**, ensure that the Sentinel installer (TAR file) and the SUSE Linux High Availability Extension (SLE HAE) ISO image with valid licenses are available.
- ❒ **(Conditional) If you are using the SLES operating system with kernel version 3.0.101 or later**, you must manually load the watchdog driver on the computer. To find the appropriate watchdog driver for your computer hardware, contact your hardware vendor. To load the watchdog driver, perform the following:
  1. In the command prompt, run the following command to load the watchdog driver in the current session:

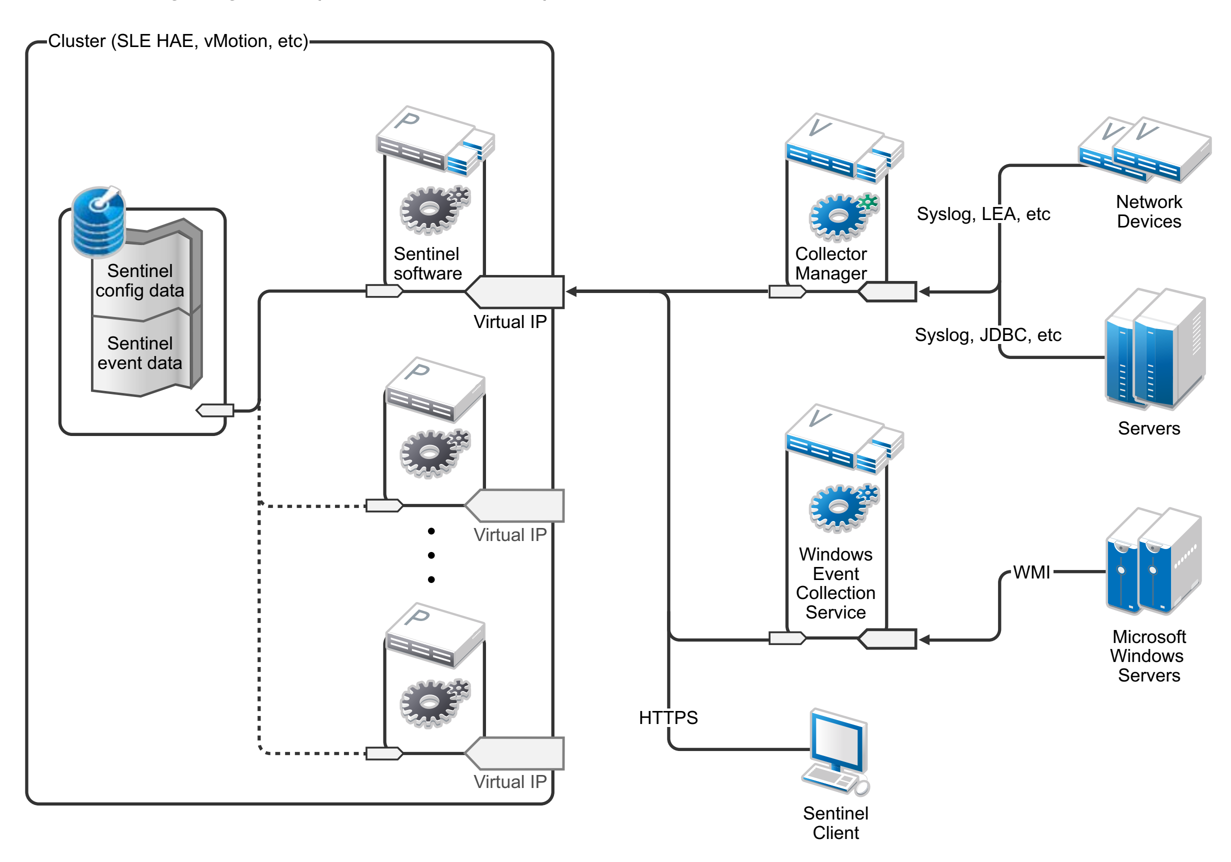
     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
  2. In the `/etc/init.d/boot.local` file, add the following line to ensure that the computer automatically loads the watchdog driver at every boot time:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Ensure that each cluster node that hosts the Sentinel services meet the requirements specified in Chapter 5, “Meeting System Requirements,” on page 37.
- ❒ Ensure that sufficient shared storage is available for the Sentinel data and application.
- ❒ Ensure that you use a virtual IP address for the services that can be migrated from node to node on failover.
- ❒ Ensure that your shared storage device meets the performance and size characteristics requirements specified in Chapter 5, “Meeting System Requirements,” on page 37. NetIQ recommends a standard SUSE Linux VM configured with iSCSI Targets as shared storage.
- ❒ Ensure that you have a minimum of two cluster nodes that meet the resource requirements for running Sentinel in the customer environment. NetIQ recommends two SUSE Linux VMs.
- ❒ Ensure you create a method for the cluster nodes to communicate with the shared storage, such as FibreChannel for a SAN. NetIQ recommends a dedicated IP address to connect to the iSCSI Target.
- ❒ Ensure you have a virtual IP that can be migrated from one node to another node in a cluster to serve as the external IP address for Sentinel.
- ❒ Ensure you have at least one IP address per cluster node for internal cluster communications. NetIQ recommends a simple unicast IP address, but multicast is preferred for production environments.

29 Installation and Configuration

This section provides the steps for installing and configuring Sentinel in a high availability (HA) environment.

The following diagram represents an active-passive HA architecture:



29.1 Initial Setup

Configure the computer hardware, network hardware, storage hardware, operating systems, user accounts, and other basic system resources per the documented requirements for Sentinel and local customer requirements. Test the systems to ensure proper function and stability.

Use the following checklist to guide you through initial setup and configuration.

	Checklist Items
❑	The CPU, RAM, and disk space characteristics for each cluster node must meet the system requirements defined in Chapter 5, “Meeting System Requirements,” on page 37 based on the expected event rate.
❑	The disk space and I/O characteristics for the storage nodes must meet the system requirements defined in Chapter 5, “Meeting System Requirements,” on page 37 based on the expected event rate and data retention policies for primary and secondary storage.
❑	If you want to configure the operating system firewalls to restrict access to Sentinel and the cluster, refer to Chapter 8, “Ports Used,” on page 53 for details of which ports must be available depending on your local configuration and the sources that will be sending event data.
❑	Ensure that all cluster nodes are time-synchronized. You can use NTP or a similar technology for this purpose.
❑	◆ The cluster requires reliable host name resolution. Enter all internal cluster host names into the `/etc/hosts` file to ensure cluster continuity in case of DNS failure. ◆ Ensure that you do not assign a host name to a loopback IP address. ◆ When configuring host name and domain name while installing the operating system, deselect **Assign Hostname to Loopback IP**.

NetIQ recommends the following configuration:

- **(Conditional) For traditional HA installations:**
  - Two SUSE Linux 11 SP3 cluster node VMs.
  - (Conditional) You can install X Windows if you require GUI configuration. Set the boot scripts to start without X (runlevel 3), so you can start them only when needed.
- **(Conditional) For HA appliance installations:** Two HA ISO appliance based cluster node VMs. For information about installing the HA ISO appliance, see Section 13.1.2, “Installing Sentinel,” on page 77.
- The nodes will have one NIC for external access and one for iSCSI communications.
- Configure the external NICs with IP addresses that allow for remote access through SSH or similar. For this example, we will use 172.16.0.1 (node01) and 172.16.0.2 (node02).
- Each node should have sufficient disk for the operating system, Sentinel binaries and configuration data, cluster software, temp space, and so forth. See the SUSE Linux and SLE HAE system requirements, and Sentinel application requirements.
- One SUSE Linux 11 SP3 VM configured with iSCSI Targets for shared storage
  - (Conditional) You can install X Windows if you require GUI configuration. Set the boot scripts to start without X (runlevel 3), so you can start them only when needed.
  - The system will have two NICs: one for external access and one for iSCSI communications.

* Configure the external NIC with an IP address that allows for remote access using SSH or similar. For example, 172.16.0.3 (storage03).
* The system should have sufficient space for the operating system, temp space, a large volume for shared storage to hold Sentinel data, and a small amount of space for an SBD partition. See the SUSE Linux system requirements, and Sentinel event data storage requirements.

NOTE: In a production cluster, you can use internal, non-routable IPs on separate NICs (possibly a couple, for redundancy) for internal cluster communications.

29.2 Shared Storage Setup

Set up your shared storage and make sure that you can mount it on each cluster node. If you are using FibreChannel and a SAN, you might need to provide physical connections as well as additional configuration. Sentinel uses this shared storage to store the databases and event data. Ensure that the shared storage is appropriately sized accordingly based on the expected event rate and data retention policies.

Example Shared Storage Setup

A typical implementation might use a fast SAN attached using FibreChannel to all the cluster nodes, with a large RAID array to store the local event data. A separate NAS or iSCSI node might be used for the slower secondary storage. As long as the cluster node can mount the primary storage as a normal block device, it can be used by the solution. The secondary storage can also be mounted as a block device, or could be an NFS or CIFS volume.

NOTE: NetIQ recommends that you configure your shared storage and test mounting it on each cluster node. However, the cluster configuration will handle the actual mount of the storage.

NetIQ recommends using the following procedure to create iSCSI Targets hosted by a SUSE Linux VM:

1. Connect to `storage03`, the VM you created during Initial Setup, and start a console session.
2. Use the `dd` command to create a blank file of any desired size for Sentinel primary storage:

   ```
   dd if=/dev/zero of=/localdata count=10240000 bs=1024
   ```

3. Create a 10GB file filled with zeros copied from the /`dev/zero pseudo-device` file. See the info or main page for the `dd` command for details on the command line options.
4. Repeat steps 1 through 3 to create a file for secondary storage:

   ```
   dd if=/dev/zero of=/networkdata count=10240000 bs=1024
   ```

NOTE: For this example you created two files of the same size and performance characteristics to represent the two disks. For a production deployment, you can create the primary storage on a fast SAN and the secondary storage on a slower iSCSI, NFS, or CIFS volume.

29.2.1 Configuring iSCSI Targets

Configure the files `localdata` and `networkdata` as iSCSI Targets:

1. Run YaST from the command line (or use the Graphical User Interface, if preferred): `/sbin/yast`
2. Select **Network Devices** > **Network Settings**.
3. Ensure that the **Overview** tab is selected.
4. Select the secondary NIC from the displayed list, then tab forward to Edit and press `Enter`.
5. On the **Address** tab, assign a static IP address of 10.0.0.3. This will be the internal iSCSI communications IP.
6. Click **Next**, then click **OK**.
7. On the main screen, select **Network Services** > **iSCSI Target**.
8. If prompted, install the required software (`iscsitarget RPM`) from the SUSE Linux 11 SP3 media.
9. Click **Service**, select the **When Booting** option to ensure that the service starts when the operating system boots.
10. Click **Global**, and then select **No Authentication** because the current OCF Resource Agent for iSCSI does not support authentication.
11. Click **Targets** and then click **Add** to add a new target.

    The iSCSI Target will auto-generate an ID and then present an empty list of LUNs (drives) that are available.
12. Click **Add** to add a new LUN.
13. Leave the LUN number as 0, then browse in the **Path** dialog (under Type=fileio) and select the `/localdata` file that you created. If you have a dedicated disk for storage, specify a block device, such as `/dev/sdc`.
14. Repeat steps 12 and 13, and add LUN 1 and `/networkdata` this time.
15. Leave the other options at their defaults. Click **OK** and then click **Next**.
16. Click **Next** again to select the default authentication options, then **Finish** to exit the configuration. Accept if asked to restart iSCSI.
17. Exit YaST.

NOTE: This procedure exposes two iSCSI Targets on the server at IP address 10.0.0.3. At each cluster node, ensure that it can mount the local data shared storage device.

29.2.2 Configuring iSCSI Initiators

Use the following procedure to format the devices:

1. Connect to one of the cluster nodes (node01) and start YaST.
2. Select **Network Devices** > **Network Settings**.
3. Ensure that the **Overview** tab is selected.
4. Select the secondary NIC from the displayed list, then tab forward to Edit and press Enter.
5. Click **Address**, assign a static IP address of 10.0.0.1. This will be the internal iSCSI communications IP.
6. Select **Next**, then click **OK**.

7 Click **Network Services** > **iSCSI Initiator**.

8 If prompted, install the required software (open-iscsi RPM) from the SUSE Linux 11 SP3 media.

9 Click **Service**, select **When Booting** to ensure the iSCSI service is started on boot.

10 Click **Discovered Targets**, and select **Discovery**.

11 Specify the iSCSI Target IP address (10.0.0.3), select **No Authentication**, and then click **Next**.

12 Select the discovered iSCSI Target with the IP address 10.0.0.3 and then select **Log In**.

13 Switch to automatic in the **Startup** drop-down and select **No Authentication**, then click **Next**.

14 Switch to the **Connected Targets** tab to ensure that we are connected to the target.

15 Exit the configuration. This should have mounted the iSCSI Targets as block devices on the cluster node.

16 In the YaST main menu, select **System** > **Partitioner**.

17 In the System View, you should see new hard disks (such as `/dev/sdb` and `/dev/sdc`) in the list - they will have a type of IET-VIRTUAL-DISK. Tab over to the first one in the list (which should be the primary storage), select that disk, then press Enter.

18 Select **Add** to add a new partition to the empty disk. Format the disk as a primary ext3 partition, but do not mount it. Ensure that the option Do not mount partition is selected.

19 Select **Next**, then **Finish** after reviewing the changes that will be made. Assuming you create a single large partition on this shared iSCSI LUN, you should end up with a `/dev/sdb1` or similar formatted disk (referred to as `/dev/<SHARED1>` below).

20 Go back into the partitioner and repeat the partitioning/formatting process (steps 16-19) for `/dev/sdc` or whichever block device corresponds to the secondary storage. This should result in a `/dev/sdc1` partition or similar formatted disk (referred to as `/dev/<NETWORK1>` below).

21 Exit YaST.

22 **(Conditional) If you are performing a traditional HA installation**, create a mountpoint and test mounting the local partition as follows (the exact device name might depend on the specific implementation):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

You should be able to create files on the new partition and see the files wherever the partition is mounted.

23 (Conditional) If you are performing a traditional HA installation, to unmount:

```
# umount /var/opt/novell
```

24 (Conditional) For HA appliance installations, repeat steps 1-15 to ensure that each cluster node can mount the local shared storage. Replace the node IP in step 5 with a different IP for each cluster node.

25 (Conditional) For traditional HA installations, repeat steps 1-15, 22, and 23 to ensure that each cluster node can mount the local shared storage. Replace the node IP in step 5 with a different IP for each cluster node.

29.3 Sentinel Installation

There are two options to install Sentinel: install every part of Sentinel onto the shared storage using the `--location` option to redirect the Sentinel installation to the location where you have mounted the shared storage or install only the variable application data on the shared storage.

NetIQ recommends installing Sentinel to each cluster node that can host it. After you install Sentinel the first time, you must perform a complete installation including the application binaries, configuration, and all the data stores. For subsequent installations on the other cluster nodes, you will only install the application. The Sentinel data will be available once you have mounted the shared storage.

29.3.1 First Node Installation

Traditional HA Installation

1 Connect to one of the cluster nodes (node01) and open a console window.

2 Download the Sentinel installer (a tar.gz file) and store it in `/tmp` on the cluster node.

3 Execute the following commands:

```
mount /dev/<SHARED1> /var/opt/novell

cd /tmp

tar -xvzf sentinel_server*.tar.gz

cd sentinel_server*

./install-sentinel --record-unattended=/tmp/install.props
```

4 Run through the standard installation, configuring the product as appropriate. The installation program installs the binaries, databases, and configuration files. The installation program also sets up the login credentials, configuration settings, and the network ports.

5 Start Sentinel and test the basic functions. You can use the standard external cluster node IP to access the product.

6 Shut down Sentinel and dismount the shared storage using the following commands:

```
rcsentinel stop

umount /var/opt/novell
```

This step removes the autostart scripts so that the cluster can manage the product.

```
cd /

insserv -r sentinel
```

Sentinel HA Appliance Installation

The Sentinel HA appliance includes the Sentinel software that is already installed and configured. To configure the Sentinel software for HA, perform the following steps:

1 Connect to one of the cluster nodes (node01) and open a console window.

2 Navigate to the following directory:

```
cd /opt/novell/sentinel/setup
```

3 Record the configuration:

3a Execute the following command:

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

This step records the configuration in the file `install.props`,which is required to configure the cluster resources using the `install-resources.sh` script.

3b Specify the option to select the Sentinel Configuration type.

3c Specify `2` to enter a new password.

If you specify `1`, the `install.props` file does not store the password.

4 Shut down Sentinel using the following command:

```
rcsentinel stop
```

This step removes the autostart scripts so that the cluster can manage the product.

```
insserv -r sentinel
```

5 Move the Sentinel data folder to the shared storage using the following commands. This movement allows the nodes to utilize the Sentinel data folder through shared storage.

```
mkdir -p /tmp/new
mount /dev/<SHARED1> /tmp/new
mv /var/opt/novell/sentinel /tmp/new
umount /tmp/new/
```

6 Verify the movement of the Sentinel data folder to the shared storage using the following commands:

```
mount /dev/<SHARED1>  /var/opt/novell/
umount /var/opt/novell/
```

29.3.2 Subsequent Node Installation

- "Traditional HA Installation" on page 144
- "Sentinel HA Appliance Installation" on page 144

Repeat the installation on other nodes:

The initial Sentinel installer creates a user account for use by the product, which uses the next available user ID at the time of the install. Subsequent installs in unattended mode will attempt to use the same user ID for account creation, but the possibility for conflicts (if the cluster nodes are not identical at the time of the install) does exist. It is highly recommended that you do one of the following:

- Synchronize the user account database across cluster nodes (manually through LDAP or similar), making sure that the sync happens before subsequent installs. In this case the installer will detect the presence of the user account and use the existing one.
- Watch the output of the subsequent unattended installs - a warning will be issued if the user account could not be created with the same user ID.

Traditional HA Installation

1. Connect to each additional cluster node (node02) and open a console window.
2. Execute the following commands:

```
cd /tmp

scp root@node01:/tmp/sentinel_server*.tar.gz

scp root@node01:/tmp/install.props

tar -xvzf sentinel_server*.tar.gz

./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props

cd /

insserv -r sentinel
```

Sentinel HA Appliance Installation

1. Connect to each additional cluster node (node02) and open a console window.
2. Execute the following command:

```
insserv -r sentinel
```

3. Stop Sentinel services.

```
rcsentinel stop
```

4. Remove Sentinel directory.

```
rm -rf /var/opt/novell/sentinel
```

At the end of this process, Sentinel should be installed on all nodes, but it will likely not work correctly on any but the first node until various keys are synchronized, which will happen when we configure the cluster resources.

29.4 Cluster Installation

You must install the cluster software only for traditional high availability (HA) installations. The Sentinel HA appliance includes the cluster software and does not require manual installation.

NetIQ Recommends the following procedure to set up the SUSE Linux High Availability Extension with a Sentinel-specific Resource Agents overlay:

1. Install the cluster software on each node.
2. Register each cluster node with the cluster manager.
3. Verify that each cluster node appears in the cluster management console.

   NOTE: The OCF Resource Agent for Sentinel is a simple shell script that runs a variety of checks to verify if Sentinel is functional. If you do not use the OCF Resource Agent to monitor Sentinel, you must develop a similar monitoring solution for the local cluster environment. To develop your own, review the existing Resource Agent, stored in the `Sentinelha.rpm` file in the Sentinel download package.

   ---

4. Install the core SLE HAE software according to the SLE HAE Documentation. For information about installing SLES add-ons, see the Deployment Guide.
5. Repeat step 4 on all cluster nodes. The add-on will install the core cluster management and communications software, as well as many Resource Agents that are used to monitor cluster resources.
6. Install an additional RPM to provide the additional Sentinel-specific cluster Resource Agents. The HA RPM can be found in the `novell-Sentinelha-<Sentinel_version>*.rpm` file, stored in the default Sentinel download, which you unpacked to install the product.
7. On each cluster node, copy the `novell-Sentinelha-<Sentinel_version>*.rpm` file into the `/tmp` directory, then run the following commands:

```
cd /tmp

rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

29.5 Cluster Configuration

You must configure the cluster software to register each cluster node as a member of the cluster. As part of this configuration, you can also set up fencing and Shoot The Other Node In The Head (STONITH) resources to ensure cluster consistency.

NetIQ Recommends the following procedure for cluster configuration:

For this solution you must use private IP addresses for internal cluster communications, and use unicast to minimize the need to request a multicast address from a network administrator. You must also use an iSCSI Target configured on the same SUSE Linux VM that hosts the shared storage to serve as a Split Brain Detection (SBD) device for fencing purposes.

SBD Setup

1. Connect to `storage03` and start a console session. Use the `dd` command to create a blank file of any desired size:

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. Create a 1MB file filled with zeros copied from the `/dev/zero` pseudo-device.
3. Run YaST from the command line or the Graphical User Interface: `/sbin/yast`

4 Select **Network Services** > **iSCSI Target**.
5 Click **Targets** and select the existing target.
6 Select **Edit**. The UI will present a list of LUNs (drives) that are available.
7 Select **Add** to add a new LUN.
8 Leave the LUN number as 2. Browse in the **Path** dialog and select the `/sbd` file that you created.
9 Leave the other options at their defaults, then select **OK** then **Next**, then click **Next** again to select the default authentication options.
10 Click **Finish** to exit the configuration. Restart the services if needed. Exit YaST.

NOTE: The following steps require that each cluster node be able to resolve the hostname of all other cluster nodes (the file sync service csync2 will fail if this is not the case). If DNS is not set up or available, add entries for each host to the `/etc/hosts` file that list each IP and its hostname (as reported by the hostname command). Also, ensure that you do not assign a hostname to a loopback IP address.

Perform the following steps to expose an iSCSI Target for the SBD device on the server at IP address 10.0.0.3 (storage03).

Node Configuration

Connect to a cluster node (node01) and open a console:

1 Run YaST.
2 Open **Network Services** > **iSCSI Initiator**.
3 Select **Connected Targets**, then the iSCSI Target you configured above.
4 Select the **Log Out** option and log out of the Target.
5 Switch to the **Discovered Targets** tab, select the **Target**, and log back in to refresh the list of devices (leave the **automatic** startup option and **No Authentication**).
6 Select **OK** to exit the iSCSI Initiator tool.
7 Open **System** > **Partitioner** and identify the SBD device as the 1MB IET-VIRTUAL-DISK. It will be listed as **/dev/sdd** or similar - note which one.
8 Exit YaST.
9 Execute the command `ls -l /dev/disk/by-id/` and note the device ID that is linked to the device name you located above.
10 Execute the command `sleha-init`.
11 When prompted for the network address to bind to, specify the external NIC IP (172.16.0.1).
12 Accept the default multicast address and port. We will override this later.
13 Enter 'y' to enable SBD, then specify `/dev/disk/by-id/<device id>`, where `<device id>` is the ID you located above (you can use Tab to auto-complete the path).
14 Complete the wizard and make sure no errors are reported.
15 Start YaST.
16 Select **High Availability** > **Cluster** (or just Cluster on some systems).
17 In the box at left, ensure **Communication Channels** is selected.
18 Tab over to the top line of the configuration, and change the **udp** selection to **udpu** (this disables multicast and selects unicast).
19 Select to **Add a Member Address** and specify this node (172.16.0.1), then repeat and add the other cluster node(s): 172.16.0.2.

20 Select **Finish** to complete the configuration.

21 Exit YaST.

22 Run the command `/etc/rc.d/openais restart` to restart the cluster services with the new sync protocol.

Connect to each additional cluster node (node02) and open a console:

1 Run YaST.

2 Open **Network Services** > **iSCSI Initiator**.

3 Select **Connected Targets**, then the iSCSI Target you configured above.

4 Select the **Log Out** option and log out of the Target.

5 Switch to the **Discovered Targets** tab, select the **Target**, and log back in to refresh the list of devices (leave the **automatic** startup option and **No Authentication**).

6 Select **OK** to exit the iSCSI Initiator tool.

7 Run the following command: `sleha-join`

8 Enter the IP address of the first cluster node.

(Conditional) If the cluster does not start correctly, perform the following steps:

1 Manually copy `/etc/corosync/corosync.conf` from `node01` to `node02`, or run `csync2 -x -v` on `node01`, or manually set the cluster up on `node02` through YaST.

2 Run `/etc/rc.d/openais start` on `node02`

(Conditional) If the `xinetd` service does not properly add the new `csync2` service, the script will not function properly. The `xinetd` service is required so that the other node can sync the cluster configuration files down to this node. If you see errors like `csync2 run failed`, you may have this problem.

To resolve this issue, execute the `kill -HUP `cat /var/run/xinetd.init.pid` command and then re-run the `sleha-join` script.

3 Run `crm_mon` on each cluster node to verify that the cluster is running properly. You can also use 'hawk', the web console, to verify the cluster. The default login name is`hacluster` and the password is `linux`.

(Conditional) Depending on your environment, perform the following tasks to modify additional parameters:

1 To ensure that in a single node failure in your two-node cluster does not unexpectedly stop the entire cluster, set the global cluster option `no-quorum-policy` to `ignore`:

```
crm configure property no-quorum-policy=ignore
```

NOTE: If your cluster contains more than two nodes, do not set this option.

---

2 To ensure that the resource manager allows resources to run in place and move, set the global cluster option `default-resource-stickiness` to 1:

```
crm configure property default-resource-stickiness=1.
```

29.6 Resource Configuration

Resource Agents are provided by default with SLE HAE. If you do not want to use SLE HAE, you need to monitor these additional resources using an alternate technology:

- A filesystem resource corresponding to the shared storage that the software uses.
- An IP address resource corresponding to the virtual IP by which the services will be accessed.
- The PostgreSQL database software that stores configuration and event metadata.

NetIQ recommends the following for resource configuration:

NetIQ provides a `crm` script to aid in cluster configuration. The script pulls relevant configuration variables from the unattended setup file generated as part of the Sentinel installation. If you did not generate the setup file, or you wish to change the configuration of the resources, you can use the following procedure to edit the script accordingly.

1. Connect to the original node on which you installed Sentinel.

   NOTE: This must be the node on which you ran the full Sentinel install.

   ---
2. Edit the script so that it appears as follows, where `<SHARED1>` is the shared volume you created previously:

   ```
   mount /dev/<SHARED1> /var/opt/novell

   cd /usr/lib/ocf/resource.d/novell

   ./install-resources.sh
   ```
3. (Conditional) You might have issues with the new resources coming up in the cluster; run `/etc/rc.d/openais restart` on node02 if you experience this issue.
4. The `install-resources.sh` script will prompt you for a couple values, namely the virtual IP that you would like people to use to access Sentinel and the device name of the shared storage, and then will auto-create the required cluster resources. Note that the script requires the shared volume to already be mounted, and also requires the unattended installation file which was created during Sentinel install to be present (`/tmp/install.props`). You do not need to run this script on any but the first installed node; all relevant config files will be automatically synced to the other nodes.
5. If your environment varies from this NetIQ recommended solution, you can edit the `resources.cli` file (in the same directory) and modify the primitives definitions from there. For example, the recommended solution uses a simple Filesystem resource; you may wish to use a more cluster-aware cLVM resource.
6. After running the shell script, you can issue a `crm status` command and the output should look like this:

   ```
   crm status
   ```

   ```
   Last updated: Thu Jul 26 16:34:34 2012
   Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
   Stack: openais
   Current DC: node01 - partition with quorum
   Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
   2 Nodes configured, 2 expected votes
   5 Resources configured.
   ```

```
Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

7 At this point the relevant Sentinel resources should be configured in the cluster. You can examine how they are configured and grouped in the cluster management tool, for example by running crm status.

29.7 Secondary Storage Configuration

Perform the following steps to configure the secondary storage so that Sentinel can migrate event partitions to less-expensive storage:

NOTE: This process is optional and the secondary storage does not need to be high-availability in the same way that you configured the rest of the system. You can use any directory, mounted from a SAN or not, NFS, or CIFS volume.

---

1. In the Sentinel web console, in the top menu bar, click **Storage**.
2. Select **Configuration**.
3. Select one of the radio buttons under Secondary storage not configured

NetIQ recommends using a simple iSCSI Target as a network shared storage location, in much the same configuration as the primary storage. In your production environment, your storage technologies might differ.

Use the following procedure to configure the secondary storage for use by Sentinel:

NOTE: Because NetIQ recommends using an iSCSI Target for this solution, the target will be mounted as a directory for use as secondary storage. You must configure the mount as a filesystem resource similar to the way the primary storage filesystem is configured. This was not automatically set up as part of the resource installation script since there are other possible variations.

---

1. Review the steps above to determine which partition was created for use as secondary storage (`/dev/<NETWORK1>`, or something like `/dev/sdc1`). If necessary create an empty directory on which the partition can be mounted (such as `/var/opt/netdata`).
2. Set up the network filesystem as a cluster resource: use the web console or run the command:

   ```
   crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/
   dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
   ```

   where `/dev/<NETWORK1>` is the partition that was created in the Shared Storage Setup section above, and <PATH> is any local directory on which it can be mounted.
3. Add the new resource to the group of managed resources:

   ```
    crm resource stop sentinelgrp
    crm configure delete sentinelgrp
    crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb
   sentinelserver
    crm resource start sentinelgrp
   ```
4. You can connect to the node currently hosting the resources (use `crm status` or `Hawk`) and make sure that the secondary storage is properly mounted (use the `mount` command).

5 Log in to the Sentinel Web interface.

6 Select **Storage**, then select **Configuration**, then select the **SAN (locally mounted**) under Secondary storage not configured.

7 Type in the path where the secondary storage is mounted, for example `/var/opt/netdata`.

NetIQ recommends using simple versions of the required resources, such as the simple Filesystem Resource Agent - customers can choose to use more sophisticated cluster resources like cLVM (a logical-volume version of the filesystem) if they wish.

30 Upgrading Sentinel in High Availability

When you upgrade Sentinel in an HA environment, you should first upgrade the passive nodes in the cluster, then upgrade the active cluster node.

30.1 Prerequisites

- Download the latest installer from the NetIQ download Web site.
- If you are using the SLES operating system with kernel version 3.0.101 or later, you must manually load the watchdog driver in the computer. To find the appropriate watchdog driver for your computer hardware, contact your hardware vendor. To load the watchdog driver, perform the following:
  1. In the command prompt, run the following command to load the watchdog driver in the current session:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. Add the following line to the `/etc/init.d/boot.local` file to ensure that the computer automatically loads the watchdog driver at every boot time:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

30.2 Upgrading a Traditional Sentinel HA Installation

1 Enable the maintenance mode on the cluster:

```
crm configure property maintenance-mode=true
```

Maintenance mode helps you to avoid any disturbance to the running cluster resources while you update Sentinel. You can run this command from any cluster node.

2 Verify whether the maintenance mode is active:

```
crm status
```

The cluster resources should appear in the unmanaged state.

3 Upgrade the passive cluster node:

3a Stop the cluster stack:

```
rcopenais stop
```

Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

3b Log in as `root` to the server where you want to upgrade Sentinel.

3c Extract the install files from the tar file:

```
tar xfz <install_filename>
```

3d Run the following command in the directory where you extracted the install files:

```
./install-sentinel --cluster-node
```

3e After the upgrade is complete, restart the cluster stack:

```
rcopenais start
```

Repeat Step 3 for all passive cluster nodes.

3f Remove the autostart scripts so that the cluster can manage the product.

```
cd /
```

```
insserv -r sentinel
```

4 Upgrade the active cluster node:

4a Back up your configuration, then create an ESM export.

For more information about backing up data, see "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide*.

4b Stop the cluster stack:

```
rcopenais stop
```

Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

4c Log in as `root` to the server where you want to upgrade Sentinel.

4d Run the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

4e Run the following command in the directory where you extracted the install files:

```
./install-sentinel
```

4f After the upgrade is complete, start the cluster stack:

```
rcopenais start
```

4g Remove the autostart scripts so that the cluster can manage the product.

```
cd /
```

```
insserv -r sentinel
```

4h Run the following command to synchronize any changes in the configuration files:

```
run csync2 -x -v
```

5 Disable the maintenance mode on the cluster:

```
crm configure property maintenance-mode=false
```

You can run this command from any cluster node.

6 Verify whether the maintenance mode is inactive:

```
crm status
```

The cluster resources should appear in the Started state.

7 (Optional) Verify whether the Sentinel upgrade is successful:

```
rcsentinel version
```

30.3 Upgrading a Sentinel HA Appliance Installation

You can upgrade a Sentinel HA appliance installation by using the Zypper patch and also through WebYast.

- Section 30.3.1, “Upgrading Sentinel HA Appliance by Using Zypper,” on page 153
- Section 30.3.2, “Upgrading Sentinel HA Appliance Through WebYast,” on page 154

30.3.1 Upgrading Sentinel HA Appliance by Using Zypper

You must register all the appliance nodes through WebYast before the upgrade. For more information, see Section 13.3.3, “Registering for Updates,” on page 83. If you do not register the appliance, Sentinel displays a yellow warning.

1 Enable the maintenance mode on the cluster.

```
crm configure property maintenance-mode=true
```

Maintenance mode helps you to avoid any disturbance to the running cluster resources while you update the Sentinel software. You can run this command from any cluster node.

2 Verify whether the maintenance mode is active.

```
crm status
```

The cluster resources should appear in the unmanaged state.

3 Upgrade the passive cluster node:

3a Download updates for the Sentinel HA appliance.

```
zypper -v patch -d
```

This command downloads updates for packages installed on the appliance including Sentinel to `/var/cache/zypp/packages`.

3b Stop the cluster stack.

```
rcopenais stop
```

Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

3c After you download the updates, install the updates using the following command:

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/
noarch/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/
rpm/x86_64/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-
Updates/rpm/i586/*.rpm --excludepath=/var/opt/novell/
```

3d Run the following script to complete the upgrade process:

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-
overlay_files.sh
```

3e After the upgrade is complete, restart the cluster stack.

```
rcopenais start
```

Repeat Step 3 for all the passive cluster nodes.

4 Upgrade the active cluster node:

4a Back up your configuration, then create an ESM export.

For more information on backing up data, see "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide*.

4b Stop the cluster stack.

```
rcopenais stop
```

Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

4c Log in to the Sentinel appliance as an administrator.

4d To upgrade the Sentinel appliance, click **Appliance** to launch WebYaST.

4e To check whether there are any updates, click **Updates**.

4f Select and apply the updates.

The updates might take few minutes to complete. After the update is successful, the WebYaST login page appears.

Before upgrading the appliance, WebYaST automatically stops the Sentinel service. You must manually restart this service after the upgrade is complete.

4g Clear your Web browser cache to view the latest Sentinel version.

4h After the upgrade is complete, restart the cluster stack.

```
rcopenais start
```

4i Run the following command to synchronize any changes in the configuration files:

```
run csync2 -x -v
```

5 Disable the maintenance mode on the cluster.

```
crm configure property maintenance-mode=false
```

You can run this command from any cluster node.

6 Verify whether the maintenance mode is inactive.

```
crm status
```

The cluster resources should appear in the Started state.

7 (Optional) Verify whether the Sentinel upgrade is successful:

```
rcsentinel version
```

30.3.2 Upgrading Sentinel HA Appliance Through WebYast

You must register all the appliance nodes through WebYast before the upgrade. For more information, see Section 13.3.3, "Registering for Updates," on page 83. If you do not register the appliance, Sentinel displays a yellow warning.

1 Enable the maintenance mode on the cluster.

```
crm configure property maintenance-mode=true
```

Maintenance mode helps you to avoid any disturbance to the running cluster resources while you update the Sentinel software. You can run this command from any cluster node.

2 Verify whether the maintenance mode is active.

```
crm status
```

The cluster resources should appear in the unmanaged state.

3 Upgrade the passive cluster nodes:

3a Stop the cluster stack.

```
rcopenais stop
```

Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

3b Specify the URL of passive cluster node using port 4984 to launch WebYaST as `https://<IP_address>:4984`, where `<IP_address>` is the IP address of passive cluster node. Log in to the Sentinel appliance as an administrator.

3c To check whether there are any updates, click **Updates**.

3d Select and apply the updates.

The updates might take few minutes to complete. After the update is successful, the WebYaST login page appears.

3e After the upgrade is complete, restart the cluster stack.

```
rcopenais start
```

Repeat Step 4 for all passive cluster nodes.

4 Upgrade the active cluster node:

4a Back up your configuration, then create an ESM export.

For more information on backing up data, see “Backing Up and Restoring Data” in the *NetIQ Sentinel Administration Guide*.

4b Stop the cluster stack.

```
rcopenais stop
```

Stopping the cluster stack ensures that the cluster resources remain accessible and avoids fencing of nodes.

4c Log in to the Sentinel appliance as an administrator.

4d To upgrade the Sentinel appliance, click **Appliance** to launch WebYaST.

4e To check whether there are any updates, click **Updates**.

4f Select and apply the updates.

The updates might take few minutes to complete. After the update is successful, the WebYaST login page appears.

Before upgrading the appliance, WebYaST automatically stops the Sentinel service. You must manually restart this service after the upgrade is complete.

4g Clear your Web browser cache to view the latest Sentinel version.

4h After the upgrade is complete, restart the cluster stack.

```
rcopenais start
```

4i Run the following command to synchronize any changes in the configuration files:

```
run csync2 -x -v
```

5 Disable the maintenance mode on the cluster.

```
crm configure property maintenance-mode=false
```

You can run this command from any cluster node.

6 Verify whether the maintenance mode is inactive.

```
crm status
```

The cluster resources should appear in the Started state.

7 (Optional) Verify whether the Sentinel upgrade is successful:

```
rcsentinel version
```

31 Backup and Recovery

The highly available failover cluster described in this document provides a level of redundancy so that if the service fails on one node in the cluster, it will automatically failover and recover on another node in the cluster. When an event like this happens, it's important to bring the node that failed back into an operational state so that the redundancy in the system can be restored and protect in the case of another failure. This section talks about restoring the failed node under a variety of failure conditions.

31.1 Backup

While a highly available failover cluster like the one described in this document provides a layer of redundancy, it is still important to regularly take a traditional backup of the configuration and data, which would not be easy to recover from if lost or corrupted. The section “Backing Up and Restoring Data” in the *NetIQ Sentinel Administration Guide* describes how to use Sentinel's built-in tools for creating a backup. These tools should be used on the active node in the cluster because the passive node in the cluster will not have the required access to the shared storage device. Other commercially available backup tools could be used instead and may have different requirements on which node they can be used.

31.2 Recovery

31.2.1 Transient Failure

If the failure was a temporary failure and there is no apparent corruption to the application and operating system software and configuration, then simply clearing the temporary failure, for example rebooting the node, will restore the node to an operational state. The cluster management user interface can be used to fail back the running service back to the original cluster node, if desired.

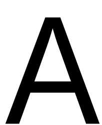
31.2.2 Node Corruption

If the failure caused a corruption in the application or operating system software or configuration that is present on the node's storage system, then the corrupted software will need to be reinstalled. Repeating the steps for adding a node to the cluster described earlier in this document will restore the node to an operational state. The cluster management user interface can be used to fail back the running service back to the original cluster node, if desired.

31.2.3 Cluster Data Configuration

If data corruption occurs on the shared storage device in a way that the shared storage device can't recover from, this would result in the corruption affecting the entire cluster in a way that cannot be automatically recovered from using the highly available failover cluster described in this document. The section "Backing Up and Restoring Data" in the *NetIQ Sentinel Administration Guide* describes how to use Sentinel's built-in tools for restoring from a backup. These tools should be used on the active node in the cluster because the passive node in the cluster will not have the required access to the shared storage device. Other commercially available backup and restore tools could be used instead and may have different requirements on which node they can be used.

VII Appendices



Troubleshooting

This section contains some of the issues that might occur during installation, along with the actions to work around the issues.

A.1 Failed Installation Because of an Incorrect Network Configuration

During the first boot, if the installer finds that the network settings are incorrect, an error message is displayed. If the network is unavailable, installing Sentinel on the appliance fails.

To resolve this issue, properly configure the network settings. To verify the configuration, use the `ifconfig` command to return the valid IP address, and use the `hostname -f` command to return the valid hostname.

A.2 The UUID Is Not Created for Imaged Collector Managers or Correlation Engine

If you image a Collector Manager server (for example, by using ZENworks Imaging) and restore the images on different machines, Sentinel does not uniquely identify the new instances of the Collector Manager. This happens because of duplicate UUIDs.

You must generate a new UUID by performing the following steps on the newly installed Collector Manager systems:

1. Delete the `host.id` or `sentinel.id` file that is located in the `/var/opt/novell/sentinel/data` folder.
2. Restart the Collector Manager.

   The Collector Manager automatically generates the UUID.

A.3 Web Interface is Blank in Internet Explorer After Logging in

If the Internet Security Level is set to High, a blank page appears after logging in to Sentinel and the file download pop-up might be blocked by the browser. To work around this issue, you need to first set the security level to Medium-high and then change to Custom level as follows:

1. Navigate to **Tools > Internet Options > Security** and set the security level to **Medium-high**.
2. Make sure that the **Tools > Compatibility View** option is not selected.
3. Navigate to **Tools > Internet Options > Security tab > Custom Level**, then scroll down to the **Downloads** section and select **Enable** under the **Automatic prompting for file downloads** option.

B Uninstalling

This appendix provides information about uninstalling Sentinel and post-uninstallation tasks.

B.1 Uninstallation Checklist

Use the following checklist to uninstall Sentinel:

- ❒ Uninstall the Sentinel server.
- ❒ Uninstall the Collector Manager and Correlation Engine, if any.
- ❒ Perform post-uninstallation tasks to complete the Sentinel uninstallation.

B.2 Uninstalling Sentinel

An uninstall script is available to help you remove a Sentinel installation. Before performing a new installation, you should perform all of the following steps to ensure there are no files or system settings remaining from a previous installation.

WARNING: These instructions involve modifying operating system settings and files. If you are not familiar with modifying these system settings and files, please contact your system administrator.

B.2.1 Uninstalling the Sentinel Server

Use the following steps to uninstall the Sentinel server:

1 Log in to the Sentinel server as `root`.

NOTE: You cannot uninstall Sentinel server as a non-root user, if the installation is performed as a `root` user. However, a non-root user can uninstall the Sentinel server if the installation was performed by non-root user.

---

2 Access the following directory:

```
/opt/novell/sentinel/setup/
```

3 Run the following command:

```
./uninstall-sentinel
```

4 When prompted to reconfirm that you want to proceed with the uninstall, press y.

The script first stops the service and then removes it completely.

B.2.2 Uninstalling the Collector Manager and Correlation Engine

Use the following steps to uninstall the Collector Manager and Correlation Engine:

1 Log in as `root` to the Collector Manager and Correlation Engine computer.

NOTE: You can not uninstall the remote Collector Manager or remote Correlation Engine as a non-root user, if the installation was performed as a `root` user. However, a non-root user can uninstall, if the installation was done as a non-root user.

---

2 Go to the following location:

```
/opt/novell/sentinel/setup
```

3 Run the following command:

```
./uninstall-sentinel
```

The script displays a warning that the Collector Manager or Correlation Engine, and all associated data will be completely removed.

4 Enter y to remove the Collector Manager or Correlation Engine.

The script first stops the service and then removes it completely. However, the Collector Manager and Correlation Engine icon is still displayed in inactive state in the Web interface.

5 Perform the following additional steps to manually delete the Collector Manager and Correlation Engine in the Web interface:

Collector Manager:

1. Access **Event Source Management > Live View**.
2. Right-click the Collector Manager you want to delete, then click **Delete**.

Correlation Engine:

1. Log in to the Sentinel Web interface as an administrator.
2. Expand **Correlation**, then select the Correlation Engine that you want to delete.
3. Click the **Delete** button (garbage can icon).

B.2.3 Uninstalling the NetFlow Collector Manager

Use the following steps to uninstall the NetFlow Collector Manager:

1 Log in to the NetFlow Collector Manager computer.

NOTE: You must log in with the same user permission that was used to install the NetFlow Collector Manager.

---

2 Change to the following directory:

```
/opt/novell/sentinel/setup
```

3 Run the following command:

```
./uninstall-sentinel
```

4 Enter `y` to uninstall the Collector Manager.

The script first stops the service and then uninstalls it completely.

B.3 Post-Uninstallation Tasks

Uninstalling the Sentinel server does not remove the Sentinel Administrator User from the operating system. You must manually remove that user.

After you uninstall Sentinel, certain systems settings remain.These settings should be removed before performing a “clean” installation of Sentinel, particularly if the Sentinel uninstallation encountered errors.

To manually clean up the Sentinel system settings:

1. Log in as `root`.
2. Ensure that all Sentinel processes are stopped.
3. Remove the contents of `/opt/novell/sentinel` or wherever the Sentinel software was installed.
4. Make sure no one is logged in as the Sentinel Administrator operating system user (novell by default), then remove the user, the home directory, and the group.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```

5. Restart the operating system.